PCT RU99/00264

РОССИЙСКОЕ АГЕНТСТВО ПО ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ
(РОСПАТЕНТ)
ФЕДЕРАЛЬНЫЙ ИНСТИТУТ ПРОМЫШЛЕННОЙ СОБСТВЕННОСТИ

рег.No 20/14-597(21)

04 ноября 1999 года

4 RU99/264

С П Р А В К А

Федеральный институт промышленной собственности Российского Агентства по патентам и товарным знакам настоящим удостоверяет, что приложенные материалы являются точным воспроизведением первоначального описания, формулы и чертежей (если имеются) заявки на выдачу патента на изобретение N 98120922, поданной в ноябре месяце 25 дня 1998 года.

Название изобретения: Способ проведения платежей и устройство для его реализации (варианты).

Заявитель (и): Закрытое акционерное общество «Алкорсофт» (ЗАО «Алкорсофт»)

Действительный автор(ы): ЗОЛОТАРЕВ Олег Анатольевич
КУЗНЕЦОВ Иван Владимирович
МОШОНКИН Андрей Геннадьевич
СМИРНОВ Александр Леонидович
ХАМИТОВ Ильдар Магафурович

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

Уполномоченный заверить копию заявки на изобретение

Г.Ф.Востриков
Заведующий отделом

7 МПК G07F 19/00
6 МПК H04L 9/00
6 МПК G07D 7/00

СПОСОБ ПРОВЕДЕНИЯ ПЛАТЕЖЕЙ И УСТРОЙСТВО ДЛЯ ЕГО РЕАЛИЗАЦИИ (варианты)

Изобретение относится к области торговых систем, электронных систем массового обслуживания, платежных систем и коммуникационных систем, и может быть использовано для организации торговли ценными бумагами, банков и банковских систем, магазинов, сервисных центров, лотерей и т.п.

Известен способ проведения платежей, описанный в патенте США [2], сущность которого состоит в том, что плательщик получает в банке посредством операции изготовления вслепую цифровой подписи данные для изготовления платежных сертификатов, которые содержат в скрытой форме идентификатор плательщика и которыми он расплачивается с другими участниками платежной системы. При этом защита от кратного использования платежных сертификатов обеспечивается тем, что идентификатор плательщика, допустившего кратное использование, может быть раскрыт. Однако, этот способ не обеспечивает предотвращения кратного использования, так безопасность банка и иных участников платежной системы зависит от поведения третьих лиц.

С целью упрощения текста данной заявки заявитель приводит пояснительные материалы об используемых в тексте понятиях, известных из опубликованных источников, а также вводит условные обозначения, идентичные по смыслу развернутым подробным понятиям и определениям, которые будут встречаться многократно на протяжении всего текста, что, по мнению заявителя, более удобно для его прочтения. В пояснительных материалах приведены, в частности, сведения о понятиях, связанных с цифровыми подписями.

Известен способ проведения платежей, описанный в патенте США [3], сущность которого состоит в том, что плательщик получает в банке цифровые подписи платежных сертификатов, называемых электронными монетами, которые он может использовать как для обмена на новые электронные монеты, так и для платежа. При этом банк не знает в каком из этих двух режимов действует плательщик, что способствует непрослеживаемости платежей. При этом защита от кратного использования электронных монет обеспечивается онлайновой проверкой получателем платежа полученных электронных монет в банке. Однако известный способ не обеспечивает полной непрослеживаемости такого участника системы, который в основном платит, а не получает платежи, так как электронные монеты, выданные такому участнику и предъявленные магазином для обмена, свидетельствуют, вообще говоря, о проведении платежа данным участником данному магазину.

В пояснительных материалах приведены сведения о понятиях, используемых заявителем при описании аналога [3].

Известен способ проведения платежей, описанный в [4], который является наиболее близким аналогом к предлагаемому изобретению и выбран заявителем в качестве прототипа. Сущность известного способа состоит в том, что клиент расплачивается сертификатами платежеспособности, называемыми электронными монетами, подписи которых он получает в банке. При этом заранее фиксируется набор возможных номиналов, а для каждого возможного номинала электронной монеты банк создает секретный и открытый денежные ключи. Для получения электронной монеты плательщик выбирает ее номер посредством датчика случайных чисел и с помощью процедуры изготовления вслепую цифровой подписи в банке, желающем прокредитовать плательщика на соответствующую сумму, получает в качестве подписи платежного сертификата цифровую подпись выбранного номера. При платеже плательщик передает получателю набор электронных монет, а получатель, проверив их правильность, пересылает полученные монеты в банк для зачисления на свой счет. Банк, проверив правильность электронных монет, зачисляет соответствующую сумму на счет получателя платежа, если монеты не были использованы ранее. Для проверки использованности банк хранит список номеров использованных монет, причем, встроенные в номера монет сроки действия позволяют удалять из списка старые номера.

Недостатки известного способа состоят в том, что деньги клиента не защищены от нечестного банка, а репутация банка не защищена от нечестных клиентов, так как получив сертификат на проверку нечестный банк может заявить, что этот сертификат уже предъявлялся ранее. В свою очередь, нечестный клиент, получив отказ банка признать уже использованный сертификат второй раз, может обвинить банк в нечестности. Кроме того, банк вынужден хранить в оперативных базах данных информацию о каждом из использованных сертификатов, что приводит к быстрому росту баз данных банка и к необходимости введения временных ограничений на действие сертификатов. Помимо этого, в известном способе сумма платежа является целочисленной комбинацией номиналов монет, что либо ограничивает диапазон платежей, либо ведет к росту числа используемых при платежах монет, что ведет к росту баз данных в банке и замедлению платежей.

Недостатки прототипа устраняются предложенными вариантами заявленного способа проведения платежей.

Известно устройство для проведения платежей описанное в патенте США [1], наиболее близкое к заявляемому устройству и выбранное заявителем в качестве прототипа.

Известное устройство состоит из платежного устройства, магазина и банка, соединенных посредством телекоммуникационных сетей, причем платежное устройство содержит блоки маскировки и демаскировки, а банк содержит блок денежной подписи, предназначенные для изготовления вслепую денежной подписи платежных сертификатов. Кроме того, магазин содержит блок, предназначенный для оффлайновой проверки платежных сертификатов, а банк содержит устройство для выявления злоумышленника в случае кратного использования им обязательства банка.

Недостатки известного устройства состоят в том, что оно не предотвращает кратное использование обязательств банка, а также медленной скорости его работы, что вызвано большим размером передаваемых по коммуникационным сетям данных.

Недостатки прототипа устраняются заявленным устройством для реализации способа проведения платежей.

Основной задачей, решаемой вариантами заявленного изобретения, является создание таких способа проведения платежей и устройства для его реализации, которые обеспечили бы эффективный и надежный механизм расплаты по открытым коммуникационным сетям, защиту каждого участника платежной системы от

злоупотреблений всех других участников, защиту приватности рядовых участников платежей, широкий диапазон платежей.

Единый для всех предложенных вариантов заявленного изобретения технический результат, достигаемый при их реализации, состоит в том, что при проведении платежей по открытым телекоммуникационным сетям денежные интересы каждого участника защищены от злоупотреблений всех других участников, причем плательщики и получатели платежей имеют возможность защиты своей приватности. Помимо этого, в некоторых из заявленных вариантов, доступны платежи в диапазоне от микроплатежей до платежей бизнес-уровня, время проведения платежа зависит только от быстроты действия сетевых соединений, но не от суммы платежа, число клиентов, которые могут быть обслужены оператором платежной системы, растет пропорционально его ресурсам.

Существенное отличие заявленного изобретения от известного уровня техники и прототипа заключается в том, что помимо защиты приватности участников платежа обеспечена защита денежных интересов плательщика тем, что платеж проводится на основании его платежного поручения, подписанного связанным с платежным сертификатом секретным ключом. Помимо этого, в некоторых из заявленных вариантов, допускается постепенное расходование платежных сертификатов и их пополнение.

Указанный выше технический результат при реализации изобретения достигается тем, что способ проведения платежей по первому варианту, заключающийся в выборе оператором платежной системы денежных секретных ключей и соответствующих денежных открытых ключей посредством генератора ключей, проведении по меньшей мере одной операции пополнения платежного устройства, при которой плательщик создает посредством датчика случайных чисел по меньшей мере одной основу платежного сертификата, которая включает его номер, и формирует денежный запрос, включающий замаскированный номер созданной основы платежного сертификата в качестве данных для изготовления вслепую денежной подписи, и доставляют его посредством коммуникационных сетей в платежный сервер оператора платежной системы, который по полученному денежному запросу определяет источник и сумму кредитования, создает при изготовлении вслепую денежной подписи данные для демаскировки посредством введения содержащихся в запросе данных для изготовления вслепую денежной подписи и соответствующего сумме кредитования денежного секретного ключа в подписывающее устройство и доставляет посредством коммуникационных сетей созданные данные для демаскировки в платежное устройство плательщика, после чего изготавливают подпись платежного сертификата введением доставленных данных для демаскировки в демаскирующее устройство и осуществляют проверку правильности изготовленной подписи платежного сертификата введением ее и денежного открытого ключа, соответствующего использованному оператором денежному секретному ключу, в устройство для проверки подписи, проведении по меньшей мере одной операции открытия у оператора платежной системы счета получателя платежа, проведении плательщиком по меньшей мере одной платежной операции, при которой подпись и основу используемого при платеже платежного сертификата включают в платежные данные, доставляемые получателю платежа, который формирует свое платежное поручение, включающее полученные от плательщика подпись и основу платежного сертификата, и доставляет его посредством коммуникационных сетей в платежный сервер оператора платежной системы, который по платежеспособности используемого при платеже платежного сертификата осуществляет кредитование счета получателя платежа на основе его платежного поручения, причем при проверке платежеспособности используемого при платеже платежного сертификата оператор

платежной системы проводит операцию его авторизации, при которой по наличию информации об авторизуемом платежном сертификате в информационном хранилище отказывают в авторизации, а по ее отсутствию осуществляют проверку правильности доставленной подписи платежного сертификата введением ее в устройство для проверки подписи, и в случае правильности заносят информацию об авторизуемом платежном сертификате в информационное хранилище, после чего формируют ответ оператора платежной системы на платежное поручение получателя платежа и доставляют его посредством коммуникационных сетей получателю платежа, который по ответу оператора платежной системы судит о проведении платежа, *отличается тем, что* в основу платежного сертификата дополнительно включают идентификатор открытого ключа подписи платежного сертификата, предварительно изготовленного совместно с соответствующим ему секретным ключом подписи посредством генератора ключей, причем открытый ключ подписи платежного сертификата доставляют посредством коммуникационных сетей в платежный сервер оператора платежной системы, в платежные данные дополнительно включают платежное поручение плательщика с подписью, которую предварительно получают на выходе подписывающего устройства после введения в него платежного поручения плательщика и секретного ключа подписи используемого платежного сертификата, причем в платежное поручение плательщика включают сведения о получателе платежа, условия платежа и идентификатор используемого платежного сертификата, при проведении по меньшей мере одной операции открытия у оператора платежной системы счета получателя платежа дополнительно получатель платежа посредством генератора ключей выбирает секретный ключ подписи счета и соответствующий открытый ключ подписи счета, причем открытый ключ подписи счета доставляют посредством коммуникационных сетей в платежный сервер оператора платежной системы, который связывает его с открываемым счетом, при формировании платежного поручения получателя платежа в него включают условия платежа, изготавливают подпись платежного поручения получателя платежа посредством введения его и секретного ключа подписи счета получателя платежа в подписывающее устройство, а изготовленную подпись доставляют посредством коммуникационных сетей в платежный сервер оператора платежной системы, при проведении платежной операции оператор платежной системы дополнительно включает в свой ответ на платежное поручение получателя платежа квитанцию получателя платежа, предварительно подписанную посредством введения ее и одного из секретных ключей подписи оператора платежной системы в подписывающее устройство, до кредитования получателя платежа дополнительно проверяют правильность подписи для платежного поручения плательщика посредством устройства для проверки подписи, в которое предварительно вводят платежное поручение плательщика и открытый ключ подписи используемого платежного сертификата, в информационное хранилище при авторизации платежного сертификата заносят подписанное платежное поручение плательщика, проверяют правильность подписи для платежного поручения получателя платежа посредством устройства для проверки подписи, в которое предварительно вводят платежное поручение получателя платежа и открытый ключ подписи счета получателя платежа, контролируют соответствие условий платежа, содержащихся в платежных поручениях плательщика и получателя платежа, получатель платежа по полученному ответу оператора платежной системы на свое платежное поручение осуществляет проверку правильности подписи для квитанции получателя платежа посредством введения ее и открытого ключа подписи, соответствующего использованному секретному ключу подписи оператора платежной системы в устройство для проверки подписи, по выходу которого судит о проведении платежа, и доставляет плательщику

данные, по которым плательщик судит о проведении платежа.

Указанный выше технический результат в частных случаях конкретной реализации может достигаться, кроме того, тем, что при выборе основы платежного сертификата в нее включают дополнительный номер, а проверку действительности основы платежного сертификата при проверке правильности доставленной подписи платежного сертификата осуществляют по совпадению номера платежного сертификате и преобразованного посредством вычислителя наперед заданной односторонней функции дополнительного номера, причем выбор посредством датчика случайных чисел основы платежного сертификата, удовлетворяющей выбранному критерию действительности основ платежных сертификатов, осуществляют посредством выбора односторонней функции, выбором посредством датчика случайных чисел дополнительного номера, а номер получают посредством обработки выбранного дополнительного номера выбранной односторонней функцией.

Более того, при включении основу платежного сертификата идентификатора открытого ключа подписи платежного сертификата, в качестве этого идентификатора возможно использовать сам открытый ключ подписи платежного сертификата.

Помимо этого, при включении в основу платежного сертификата идентификатор открытого ключа подписи платежного сертификата включают в основу в качестве дополнительного номера.

Кроме того, перед включением в платежные данные платежного поручение плательщика осуществляют его шифрование одним из открытых ключей для шифрования оператора платежной системы, а оператор платежной системы производит дешифрование полученного от получателя платежа платежного поручения плательщика секретным ключом оператора платежной системы, соответствующим использованному плательщиком открытому ключу для шифрования.

В частности, оператор платежной системы осуществляет шифрование своего ответа на платежное поручение получателя платежа.

Кроме того, условия платежа, содержащиеся в платежном поручении плательщика, могут включать данные обязательства получателя платежа перед плательщиком.

Помимо этого, при подготовке плательщиком платежных данных производят обработку данных обязательства получателя платежа перед плательщиком наперед заданной маскирующей функцией, а данные, полученные при этой обработке, включают в подготавливаемое платежное поручение плательщика, получатель платежа производит обработку данных обязательства получателя платежа перед плательщиком наперед заданной маскирующей функцией, а данные, полученные при этой обработке, включают в платежное поручение получателя платежа.

В частности, наперед заданную маскирующую функцию выбирают произвольно из множества односторонних функций.

Более того, получатель платежа подписывает данные обязательства получателя платежа перед плательщиком одним из своих секретных ключей для подписи, получатель платежа до платежной операции проверяет подпись получателя для данных обязательства получателя платежа перед плательщиком.

В частности, при проведении по меньшей мере одной операции пополнения платежного устройства в качестве источника кредитования используют счет плательщика, который предварительно кредитуют при по меньшей мере одной платежной операции.

Помимо этого, при проведении по меньшей мере одной операции пополнения платежного устройства в качестве источника кредитования используют банковскую карточку.

В частности, при проведении платежной операции в качестве плательщика выступает получатель платежа.

Более того, оператор платежной системы может включать по меньшей мере два платежных сервера.

Под оператором платежной системы заявитель имеет ввиду субъекта, который обеспечивает проведение расчетов участников платежей. В частности оператор платежной системы может вести счета участников платежей и эмитировать ценные документы. Оператор платежной системы может состоять из одного банка, а может включать в себя несколько организаций, в том числе и банков, которые связаны между собой различными договорными обязательствами. В частности, секретные ключи оператора платежной системы могут быть секретом одной из организаций, входящих в состав оператора платежной системы, а обязательства оператора платежной системы перед третьей стороной также могут быть обязательствами лишь одной из организаций, входящих в состав оператора платежной системы. В случае, если оператор платежной системы включает несколько платежных серверов, принадлежащих различным банкам или иным организациям, должна имеется безопасная система урегулирования взаимных обязательств между организациями, входящими в состав оператора платежной системы. Такие безопасные системы урегулирования взаимных обязательств известны специалистам среднего уровня.

Под платежным сертификатом заявитель имеет ввиду цифровые данные, представляющие обязательство оператора платежной системы. Платежный сертификата включает основу и цифровую подпись оператора платежной системы для этой основы, подтверждающую номинальную стоимость сертификата.

Под авторизацией платежного сертификата заявитель имеет ввиду процедуру признания эмитентом платежного сертификата своих обязательств по нему. Данная процедура может включать проверку эмитентом собственной подписи для авторизуемого сертификата, проверку срока годности и иных данных.

В некоторых схемах цифровой подписи легко изготовить подпись для случайных данных без знания секретных ключей подписи. Поэтому, для того, чтобы защитить оператора платежной системы от подделок подписи среди всех основ платежных сертификатов выделяют множество действительных основ. В примерах 1 и 2 приведены два критерия действительности основ платежных сертификатов.

Пример 1

Основа платежного сертификата представляет последовательность битов достаточно большой длины, причем основа считается действительной, если все нечетные биты этой последовательности равны нулю.

Пример 2

Основа платежного сертификата представлена двумя последовательностями битов X и Y, причем основа считается действительной, если $f(Y) = X$, где функция f является односторонней, то есть, в данном случае, вычислительно необратимой для всех, кроме, возможно, оператора платежной системы.

Заявитель отмечает, что цифровая подпись основы платежного сертификата может быть представлена другой цифровой подписью для части данных, входящих в основу, при условии, что имеется связь этой части данных с остальными данными основы. Например, в примере 2 цифровая подпись для основы (X,Y) может быть представлена некоторой цифровой подписью для данных X и данными Y, а при проверке правильности подписи основы, кроме проверки правильности подписи для X, проверяют и соотношение $f(Y) = X$.

Сущность способа проведения платежей по первому варианту состоит в том, что оператор платежной системы выбирает денежные секретные ключи и соответствующие

денежные открытые ключи в рамках некоторой схемы цифровой подписи, допускающей изготовление цифровой подписи вслепую. С каждым открытым денежным ключом связывается определенная номинальная стоимость, причем сами открытые ключи и соответствующие им номинальные стоимости публикуются.

Плательщик, желая пополнить свое платежное устройство, выбирает секретный ключ подписи платежного сертификата и соответствующий ему открытый ключ подписи платежного сертификата в рамках некоторой системы цифровой подписи, выбирает основу платежного сертификата, включающую его номер и идентификатор открытого ключа подписи платежного сертификата, после чего производит маскировку номера платежного сертификата в рамках некоторой схемы изготовления вслепую цифровой подписи и доставляет оператору платежной системы денежный запрос, включающий замаскированный номер, указание на источник кредитования и, возможно, сумму кредитования, если она не предусмотрена иными обстоятельствами, например условиями обслуживания указанного источника кредитования. Например, в качестве источника кредитования может быть указан счет плательщика или его банковская карточка. Безопасность удаленного востребования ценностей с указанного источника кредитования должна быть обеспечена системой обслуживания этого источника кредитования.

Получив денежный запрос оператор платежной системы по этому запросу определяет источник и сумму кредитования, выбирает секретный денежный ключ, соответствующий сумме кредитования, изготавливает данные для демаскировки, по которым плательщик может изготовить подпись платежного сертификата и доставляет изготовленные данные для демаскировки плательщику. При этом платежеспособность источника кредитования уменьшается в соответствии с суммой кредитования и стоимостью данной услуги оператора платежной системы.

Получив от оператора платежной системы данные для демаскировки плательщик изготавливают подпись платежного сертификата демаскировкой полученных данных и получает тем самым годный для проведения платежной операции платежный сертификат. Приватность плательщика обеспечена тем, что подпись платежного сертификата изготовлена вслепую и, тем самым, прервана ее связь с источником кредитования.

Для получения платежа получатель открывает у оператора платежной системы счет, допускающий безопасное удаленное управление. Для этого получатель платежа выбирает секретный ключ подписи счета и соответствующий открытый ключ подписи счета, в рамках некоторой схемы цифровой подписи, и доставляет открытый ключ подписи счета оператору платежной системы, который открывает счет и связывает его с полученным открытым ключом подписи счета. В дальнейшем оператор платежной системы проводит операции с данным счетом, руководствуясь подписанными указаниями, подпись для которых проверяется открытым ключом подписи счета. Безопасность владельца счета обеспечивается тем, что оператор платежной системы отчитывается перед владельцем счета подписанными указаниями. Для удобства счету может быть присвоен номер, который сообщается владельцу счета. Субъект, открывающий счет у оператора платежной системы, считает счет открытым только после получения подписанного оператором платежной системы сообщения, которое подтверждает открытие счета, связанного с открытым ключом подписи счета.

Плательщик, имея годный платежный сертификат и желая заплатить получателю платежа соответствующую стоимость, готовит платежные данные, включающие предназначенное для оператора платежной системы платежное поручение плательщика и , возможно, данные, предназначенные для получателя платежа. Данные, предназначенные для получателя платежа, могут включать указание услуги или товара,

которые оплачивает плательщик. В платежное поручение плательщика включают основу платежного сертификата, сведения о счете получателя платежа, если этот счет не определен иными обстоятельствами, и условия платежа. Условия платежа могут содержать, возможно в скрытой от оператора платежной системы форме, обязательства, накладываемые на получателя платежа фактом его проведения. При этом платежное поручение плательщика подписывается секретным ключом подписи платежного сертификата. Подготовленные платежные данные доставляют получателю платежа.

Получатель платежа, желая принять платеж, формирует свое платежное поручение, включающее полученное платежное поручение плательщика и условия платежа, подписывает его секретным ключом подписи того счета, на который он принимает платеж и доставляет оператору платежной системы.

Оператор платежной системы при наличии записи о платежном сертификате, основа которого содержится в платежном поручении плательщика, в поддерживаемом им списке использованных платежных сертификатов, считает данный платежный сертификат использованным и отказывает в его авторизации. Платеж также не проводится, если не верна подпись платежного поручения плательщика, проверяемая содержащимся в присланной основе платежного сертификата открытым ключом подписи, или не верна подпись для полученного платежного поручения получателя платежа, проверяемая открытым ключом подписи счета получателя платежа, а также если условия платежа, содержащихся в платежных поручениях плательщика и получателя платежа не соответствуют друг другу. Если же все эти условия проведения платежа выполнены, то оператор платежной системы, проверив правильность подписи платежного сертификата, заносит в список использованных платежных сертификатов сведения о данном платежном сертификате вместе с подписанным платежным поручением плательщика, кредитует на соответствующую номинальной стоимости сумму счет получателя платежа, сохранив при этом подписанное поручение получателя платежа, и доставляет получателю платежа ответ оператора платежной системы на платежное поручение получателя платежа, включающий подписанную оператором платежной системы квитанцию получателя платежа.

Получатель платежа, проверив правильность подписи оператора платежной системы для квитанции получателя платежа, считает платеж проведенным, и доставляет плательщику данные, подтверждающие проведение платежа.

Единая совокупность признаков первого варианта заявленного способа, перечисленных выше, связана причинно-следственной связью с ранее изложенным техническим результатом изобретения, заключающемся в том, что при проведении платежей по открытым телекоммуникационным сетям денежные интересы каждого участника защищены от злоупотреблений всех других участников, причем плательщики и получатели платежей имеют возможность защиты своей приватности.

Указанный выше технический результат при осуществлении способа проведения платежей по первому варианту достигается, в частности, тем, что плательщик защищен от нечестного оператора платежной системы тем, что последний обязан отчитываться о проведенных им расходах по платежному сертификату подписанным платежным поручением плательщика, приватность плательщика защищена процедурой изготовления подписи платежного сертификата вслепую, а приватность получателя платежа может быть защищена тем, что при открытии счета получатель платежа не обязан сообщать никаких сведений, позволяющих определить его личность.

Ниже заявитель приводит примеры конкретной реализации отдельных операций, а также пример полной реализации способа проведения платежей по первому варианту.

Пример 3

Денежные секретные и соответствующие денежные открытые ключи в рамках схемы цифровой подписи, допускающей изготовление цифровой подписи вслепую, могут быть выбраны следующим образом. Выбирается RSA-модуль N как произведение двух простых чисел P и Q и выбираются взаимно простые открытые экспоненты E1, E2, E3. Способы выбора таких данных хорошо известны [12], [13]. Открытым денежным ключом является набор данных (N, E), где открытая экспонента E представлена как произведение открытых экспонент E1, E2, E3 в натуральных степенях M1, M2, M3.

Также заранее выбираются номинальные стоимости S1, S2, S3, связанные с открытыми экспонентами E1, E2, E3, а с открытой экспонентой E связывается номинальная стоимость S = M1×S1 + M2×S2 +M3×S3. Для определенности, в данном примере, M1 = 1 рубль, M2 = 100 рублей, M3 = 1000 рублей.

Оператор платежной системы, который в данном примере является банком, фиксирует публичную одностороннюю функцию F, принимающую значения в натуральных числах не превосходящих N. В качестве такой функции можно взять одну из признанных хэш-функций (см.[12], [13]), рассматривая ее образ как двоичное разложение целого числа. Вычислители таких функций, то есть средства для их вычисления, также хорошо известны.

Основой платежного сертификата являются данные (Y, X), где F(Y)=X. При этом X номером платежного сертификата, а Y идентификатором открытого ключа подписи платежного сертификата. При выборе основы платежного сертификата плательщик выбирает секретный ключ подписи DP и соответствующий ему открытый ключ подписи EP и в рамках произвольной схемы цифровой подписи, и получает основу платежного сертификата (Y, X), где Y = EP, а X = F(EP). Для определенности в данном примере DP и EP являются RSA-ключами.

Пример 4

В этом примере используются обозначения и соглашения, принятые в примере 3. Плательщик, желая получить для основы платежного сертификата (Y, X) подпись, соответствующую номиналу 320 рублей, производит маскировку номера X способом известным из [6] в соответствии с открытой экспонентой E и степенями M1= 20, M2=3, M3=0, удовлетворяющими соотношению 320 = M1×S1 + M2×S2 +M3×S3. и получает замаскированные данные X', которые доставляет в банк вместе с номером своего счета и суммой кредитования 320 рублей в качестве денежного запроса.

Банк выбирает секретный денежный ключ, соответствующий сумме кредитования в 320 рублей, выбирая секретную экспоненту D как произведение секретных экспонент D1, D2, D3, соответствующих открытым экспонентам E1, E2, E3, в степенях M1, M2, M3. После этого банк изготавливает данные для демаскировки SIGN' способом известным из [6], и производит дебетование указанного плательщиком счета на 321 рубль в предположении, что стоимость услуги по изготовлению подписи равна 1 рублю.

Получив данные для демаскировки SIGN' плательщик изготавливают подпись платежного сертификата SIGN демаскировкой полученных данных SIGN' способом известным из [6] и получает тем самым годный для проведения платежной операции платежный сертификат номинальной стоимостью 320 рублей.

Пример 5

В этом примере используются обозначения и соглашения, принятые в примере 3. Получатель платежа, являющийся в данном примере продавцом, открывает в банке счет, допускающий безопасное удаленное управление. Для этого продавец выбирает секретный ключ и открытый ключи подписи счета подписи счета DS и ES, в рамках

произвольной схемы цифровой подписи, и доставляет ключ ES по открытой сети в банк. Банк присваивает открываемому счету номер No1 и создает в хранилище счетов запись, содержащую данные ES, No1 и иные атрибуты счета. Подписанные банком данные счета доставляются по открытой сети продавцу, который, проверив подпись банка, считает счет открытым.

Пример 6

В этом примере используются обозначения и соглашения, принятые в примерах 4, 5.

Плательщик, желая заплатить продавцу 320 рублей за некоторый товар готовит платежные данные PaymentData = (PayerOrder, A), где PayerOrder платежное поручение плательщика, подписанное секретным ключом подписи платежного сертификата DP,а данные A предназначены для продавца и состоят в данном примере из наименования оплачиваемого товара и идентификационных данных лица, которому следует выдать данный товар. Платежное поручение плательщика PayerOrder состоит из открытого ключ подписи платежного сертификата EP, подписи платежного сертификата SIGN, номера счета получателя платежа No1, и данных C, определяющих условия платежа C. В данном примере в качестве C плательщик берет номер счета продавца No1 и образ заранее оговоренной хэш-функции H от текста обязательства, которое принимает на себя продавец в случае проведения платежа, а именно обязательства предоставить соответствующий товар лицу с указанными идентификационными данными.

Получатель платежа, желая принять платеж, формирует свое платежное поручение SellerOrder = (No1, C, PaymentData), подписанное секретным ключом DS, и доставляет его в банк.

Ниже заявитель приводит пример конкретной реализации способа проведения платежей по первому варианту.

Пример 7

В этом примере используются обозначения и соглашения, принятые в примере 6.

Банк выбирает денежные ключи, а плательщик выбирает основу платежного сертификата как в примере 3. Операцию пополнения платежного устройства плательщика производят как в примере 4, продавец открывает в банке счет как в примере 5, а плательщик и продавец проводят платежную операцию как в примере 6.

Банк, убедившись, что в списке использованных платежных сертификатов отсутствует запись о платежном сертификате с открытым ключом подписи EP, проверив подпись платежного поручения плательщика PayerOrder открытым ключом открытым ключом подписи EP, проверив подпись платежного поручения продавца SellerOrder открытым ключом подписи счета No1, проверив совпадение условий платежа, содержащихся в платежных поручениях плательщика и продавца, и проверив правильность подписи платежного сертификата SIGN заносит в список использованных платежных сертификатов запись, включающую открытый ключ EP и подписанное платежное поручение плательщика PayerOrder, кредитует на счет получателя платежа на сумму 319 рублей, в предположении, что стоимость проведения платежной операции банком равна 1 рублю, сохраняет подписанное поручение получателя платежа SellerOrder в своем информационном хранилище. После этого банк формирует квитанцию продавца, подтверждающую факт кредитования счета с номером No1 на сумму 319 рублей, подписывает ее и доставляет продавцу, который, проверив правильность подписи банка для полученной квитанции, считает платеж проведенным, и сообщает плательщику об успешном проведении платежа.

В качестве других частных случаев способа по первому варианту заявитель отмечает возможность реализации в виде многих иных комбинаций зависимых пунктов 2-14, а

также возможность шифрования, дешифрования и перекодировки данных при их передаче по коммуникационным сетям, которые не меняют сущности заявленного изобретения.

Кроме того, оператор платежной системы при авторизации платежного сертификата может проверять подпись платежного сертификата как открытыми так и секретными денежными ключами. Помимо этого, при ошибках работы коммуникационных сетей при проведении вовлеченных в проведение платежа операций, такие операции могут быть повторены до их успешного завершения без ущерба для вовлеченных сторон.

Указанный выше технический результат при реализации изобретения достигается тем, что способ проведения платежей по второму варианту, заключающийся в выборе оператором платежной системы денежных секретных ключей и соответствующих денежных открытых ключей посредством генератора ключей, выборе плательщиком посредством датчика случайных чисел по меньшей мере одной основы платежного сертификата, которая содержит номер платежного сертификата, являющийся одновременно и подписью нулевого уровня платежного сертификата, проведении по меньшей мере одной операции пополнения платежного устройства, при которой плательщик создает посредством датчика случайных чисел по меньшей мере одной основу платежного сертификата, которая включает его номер, и формирует денежный запрос, включающий замаскированный номер созданной основы платежного сертификата в качестве данных для изготовления вслепую денежной подписи, и доставляют его посредством коммуникационных сетей в платежный сервер оператора платежной системы, который по полученному денежному запросу определяет источник и сумму кредитования, создает при изготовлении вслепую денежной подписи данные для демаскировки посредством введения содержащихся в запросе данных для изготовления вслепую денежной подписи и соответствующего сумме кредитования денежного секретного ключа в подписывающее устройство и доставляет посредством коммуникационных сетей созданные данные для демаскировки в платежное устройство плательщика, после чего изготавливают подпись платежного сертификата введением доставленных данных для демаскировки в демаскирующее устройство и осуществляют проверку правильности изготовленной подписи платежного сертификата введением ее и денежного открытого ключа, соответствующего использованному оператором денежному секретному ключу, в устройство для проверки подписи, проведении по меньшей мере одной операции авторизации оператором платежной системы платежного сертификата, подпись которого плательщик доставляет посредством коммуникационных сетей в платежный сервер оператора платежной системы, который осуществляет проверку правильности доставленной подписи платежного сертификата введением ее в устройство для проверки подписи, проведении по меньшей мере одной операции открытия у оператора платежной системы счета получателя платежа, проведении плательщиком по меньшей мере одной платежной операции, при которой подпись и основу используемого при платеже платежного сертификата включают в платежные данные, доставляемые получателю платежа, который формирует свое платежное поручение, включающее полученные от плательщика подпись и основу платежного сертификата, и доставляет его посредством коммуникационных сетей в платежный сервер оператора платежной системы, который по платежеспособности используемого при платеже платежного сертификата осуществляет кредитование счета получателя платежа на основе его платежного поручения, формирует свой ответ на платежное поручение получателя платежа и доставляет его получателю платежа, который по ответу оператора платежной системы судит о проведении платежа, *отличается тем, что* в основу

платежного сертификата дополнительно включают идентификатор открытого ключа подписи платежного сертификата, предварительно изготовленного совместно с соответствующим ему секретным ключом подписи посредством генератора ключей, причем открытый ключ подписи платежного сертификата доставляют посредством коммуникационных сетей в платежный сервер оператора платежной системы, который при проведении операции авторизации дополнительно осуществляет поиск платежного счета, связанного с авторизуемым им платежном сертификатом, и в случае отсутствия такого счета, открывает его, а при наличии такого счета производит его кредитование на основе уровней авторизованных платежных сертификатов, связанных с данным счетом, доставляемую оператору платежной системы подпись авторизуемого им платежного сертификата плательщик изготавливает по соответствующим этому платежному сертификату данным для получения посредством демаскировки подписи платежного сертификата, причем уровень изготавливаемой подписи выбирают произвольно в пределах уровня секретного ключа, использованного для изготовления данных для получения посредством демаскировки подписи платежного сертификата, в платежные данные дополнительно включают платежное поручение плательщика с подписью, которую предварительно получают на выходе подписывающего устройства после введения в него платежного поручения плательщика и секретного ключа подписи используемого платежного сертификата, причем в платежное поручение плательщика включают сведения о получателе платежа, условия платежа и идентификатор используемого платежного сертификата, при проведении по меньшей мере одной операции открытия у оператора платежной системы счета получателя платежа дополнительно получатель платежа выбирает посредством датчика случайных чисел секретный ключ подписи счета и соответствующий открытый ключ подписи счета, причем открытый ключ подписи счета доставляют посредством коммуникационных сетей в платежный сервер оператора платежной системы, который связывает его с открываемым счетом, при формировании платежного поручения получателя платежа в него включают условия платежа, изготавливают подпись платежного поручения получателя платежа посредством обработки его секретным ключом подписи счета получателя платежа, а изготовленную подпись доставляют посредством коммуникационных сетей в платежный сервер оператора платежной системы, при проведении платежной операции оператор платежной системы дополнительно включает в свой ответ на платежное поручение получателя платежа квитанцию получателя платежа, предварительно подписанную посредством введения ее и одного из секретных ключей подписи оператора платежной системы в подписывающее устройство, до кредитования получателя платежа дополнительно проверяют правильность подписи для платежного поручения плательщика посредством устройства для проверки подписи, в которое предварительно вводят платежное поручение плательщика и открытый ключ подписи используемого платежного сертификата, проверяют правильность подписи для платежного поручения получателя платежа посредством устройства для проверки подписи, в которое предварительно вводят платежное поручение получателя платежа и открытый ключ подписи счета получателя платежа, контролируют соответствие условий платежа, содержащихся в платежных поручениях плательщика и получателя платежа, при кредитовании счета получателя платежа дополнительно осуществляют дебетование платежного счета, связанного с используемым при платеже платежным сертификатом, получатель платежа по полученному ответу оператора платежной системы на свое платежное поручение осуществляет проверку правильности подписи для квитанции получателя платежа посредством введения ее и открытого ключа подписи, соответствующего

использованному секретному ключу подписи оператора платежной системы в устройство для проверки подписи, по выходу которого судит о проведении платежа, и доставляет плательщику данные, по которым плательщик судит о проведении платежа.

Указанный выше технический результат в частных случаях конкретной реализации может достигаться, кроме того, тем, что при выборе основы платежного сертификата в нее включают дополнительный номер, а проверку действительности основы платежного сертификата при проверке правильности доставленной подписи платежного сертификата осуществляют по совпадению номера платежного сертификате и преобразованного посредством вычислителя наперед заданной односторонней функции дополнительного номера, причем выбор посредством датчика случайных чисел основы платежного сертификата, удовлетворяющей выбранному критерию действительности основ платежных сертификатов, осуществляют посредством выбора односторонней функции, выбором посредством датчика случайных чисел дополнительного номера, а номер получают посредством обработки выбранного дополнительного номера выбранной односторонней функцией.

В частности, при включении основу платежного сертификата идентификатора открытого ключа подписи платежного сертификата, в качестве этого идентификатора используют сам открытый ключ подписи платежного сертификата.

Более того, при включении в основу платежного сертификата идентификатор открытого ключа подписи платежного сертификата включают в основу в качестве дополнительного номера.

Помимо этого, перед включением в платежные данные платежного поручение плательщика осуществляют его шифрование одним из открытых ключей для шифрования оператора платежной системы, а оператор платежной системы производит дешифрование полученного от получателя платежа платежного поручения плательщика секретным ключом оператора платежной системы, соответствующим использованному плательщиком открытому ключу для шифрования.

Кроме этого, оператор платежной системы осуществляет шифрование своего ответа на платежное поручение получателя платежа.

Более того, в условия платежа, содержащиеся в платежном поручении плательщика, включают данные обязательства получателя платежа перед плательщиком.

Помимо этого, при подготовке плательщиком платежных данных производят обработку данных обязательства получателя платежа перед плательщиком наперед заданной маскирующей функцией, а данные, полученные при этой обработке, включают в подготавливаемое платежное поручение плательщика, получатель платежа производит обработку данных обязательства получателя платежа перед плательщиком наперед заданной маскирующей функцией, а данные, полученные при этой обработке, включают в платежное поручение получателя платежа.

В частности, наперед заданную маскирующую функцию выбирают произвольно из множества односторонних функций.

Кроме этого, получатель платежа подписывает данные обязательства получателя платежа перед плательщиком одним из своих секретных ключей для подписи, получатель платежа до платежной операции проверяет подпись получателя для данных обязательства получателя платежа перед плательщиком.

В частности, при проведении по меньшей мере одной операции пополнения платежного устройства в качестве источника кредитования используют счет плательщика, который предварительно кредитуют при по меньшей мере одной платежной операции.

Кроме этого, при проведении по меньшей мере одной операции пополнения

платежного устройства в качестве источника кредитования может быть использована банковская карточка.

Помимо этого, при открытии платежного счета, связанного с авторизуемым платежном сертификатом, производят его предварительное дебетование.

В частности, при проведении платежной операции в качестве плательщика может выступать получатель платежа.

Более того, оператора платежной системы может иметь по меньшей мере два платежных сервера.

Сущность способа проведения платежей по второму варианту состоит в том же, что и по первому варианту, за исключением того, что используют многоразовые платежные сертификаты. Это выражается в том, что оператор платежной системы при проведении операции авторизации в случае отсутствия в его информационном хранилище сведений об авторизуемом платежном сертификате открывает связанный с данным платежным сертификатом платежный счет и связывает его с открытым ключом подписи платежного сертификата. В случае же наличия в информационном хранилище оператора платежной системы сведений об авторизуемом платежном сертификате, то есть записи о соответствующем платежном счете, оператор платежной системы не отвергает платеж, а проводит его в зависимости от того, покрывает ли сальдо платежного счета, то есть превышение кредита платежного счета над его дебетом, проплачиваемую сумму. Платежный счет, связанный с платежным сертификатом, кредитуется при операциях авторизации оператором платежной системы присланных плательщиком подписей платежных сертификатов в том случае, если уровень доставленной подписи платежного сертификата превышает уровень ранее авторизованной подписи данного платежного сертификата. При этом, плательщик может кредитовать свой платежный счет в ходе нескольких операций авторизации, шаг за шагом повышая известный оператору платежной системы уровень платежного сертификата. Это позволяет плательщику ослабить возможность связывания платежного сертификата с источником его кредитования по номинальной стоимости платежного сертификата. Кроме того, плательщик может использовать один и тот же платежный сертификат при нескольких платежных операциях, при некоторых из них доставляя оператору платежной системы данные для кредитования платежного счета, то есть подпись платежного сертификата более высокого уровня, чем уже известна оператору платежной системы. Такие подписи плательщик может изготовить из данных для демаскировки, полученных им при изготовлении вслепую денежной подписи. Помимо этого, сумма платежа может быть произвольной в рамках платежеспособности используемого платежного сертификата, так как ее величина не связана с номинальными стоимостями, соответствующими денежным ключам.

Под платежным счетом заявитель имеет ввиду счет, допускающий проведение с него платежей путем перевода части суммы счета на другой счет или перевода части суммы счета в иную форму для выдачи их получателю платежа.

Под уровнем платежного сертификата, а также соответствующим ему уровнем подписи и уровнем денежного ключа заявитель имеет ввиду данные, определяющие денежный ключ в частично упорядоченном множестве денежных ключей таким образом, что при сложении уровней складываются и номинальную стоимости, соответствующие этим денежным уровням.

Ниже заявитель приводит пример уровней платежных сертификатов, их подписей и соответствующих им денежных ключей.

Пример 8

В этом примере используются обозначения и соглашения, принятые в примере 3.

Уровнем денежного ключа в данном примере является набор из трех чисел (M1, M2, M3), а частичное упорядочение уровней задано покоординатным упорядочением таких наборов, то есть уровень (M1, M2, M3) больше некоторого другого уровня (K1, K2, K3), если M1 больше K1, M2 больше K2 и M3 больше K3 .

Например, уровень подписи SIGN из примера 4 равен (M1, M2, M3) = (20, 3, 0).

Единая совокупность признаков второго варианта заявленного способа, перечисленных выше, связана причинно-следственной связью с ранее изложенным техническим результатом изобретения, заключающемся в том, что при проведении платежей по открытым телекоммуникационным сетям денежные интересы каждого участника защищены от злоупотреблений всех других участников, причем плательщики и получатели платежей имеют возможность защиты своей приватности. Помимо этого доступны платежи в диапазоне от микроплатежей до платежей бизнес-уровня, время проведения платежа зависит только от быстроты действия сетевых соединений, но не от суммы платежа, число клиентов, которые могут быть обслужены оператором платежной системы, растет пропорционально его ресурсам.

Указанный выше технический результат при осуществлении способа проведения платежей по второму варианту достигается, в частности, тем, что плательщик защищен от нечестного оператора платежной системы тем, что последний обязан отчитываться о проведенных им расходах по платежному сертификату подписанным платежным поручением плательщика, приватность плательщика защищена процедурой изготовления подписи платежного сертификата вслепую, а приватность получателя платежа может быть защищена тем, что при открытии счета получатель платежа не обязан сообщать никаких сведений, позволяющих определить его личность. Диапазон платежей и независимость времени проведения платежей обеспечены независимость суммы платежа от номинальных стоимостей, соответствующих денежным ключам. Рост числа клиентов пропорционально ресурсам оператора платежной системы обеспечен тем, что с помощью одного платежного сертификата можно проводить большое число платежей, а число используемых платежных сертификатов может быть ограничено стоимостью операции открытия платежного счета и операции изготовления вслепую денежной подписи.

Ниже заявитель приводит пример конкретной реализации способа проведения платежей по второму варианту.

Пример 9

В этом примере используются обозначения и соглашения, принятые в примерах 3, 4, 5. Банк выбирает денежные ключи, а плательщик выбирает основу платежного сертификата как в примере 3. Операцию пополнения платежного устройства плательщика производят как в примере 4, продавец открывает в банке счет как в примере 5, а плательщик и продавец проводят платежную операцию как в примере 6.

Плательщик, желая заплатить продавцу 115.5 рублей за некоторый товар готовит платежные данные PaymentData = (PayerOrder, A), где PayerOrder платежное поручение плательщика, подписанное секретным ключом подписи платежного сертификата DP,а данные A предназначены для продавца и состоят в данном примере из наименования оплачиваемого товара и идентификационных данных лица, которому следует выдать данный товар. Платежное поручение плательщика PayerOrder состоит из открытого ключ подписи платежного сертификата EP, подписи платежного сертификата уменьшенного уровня sign, номера счета получателя платежа No1, и данных C,

определяющих условия платежа С как и в примере 6. Подпись платежного сертификата уменьшенного уровня sign плательщик изготавливает понижением уровня (M1, M2, M3) = (20, 3, 0) подписи SIGN. В качестве уровня подписи sign плательщик выбирает (K1, K2,) = (17, 1,0), так как соответствующий этой сумме номинал равен 117 рублей, что достаточно для проведения платежа на сумму 115.5 рублей. Подпись sign плательщик в данном примере изготавливает посредством возведения подписи SIGN в степень L, равную произведению открытых экспонент E1, E2, E3 в степенях (M1- K1, M2-K2,, M3-K3), что может быть выполнено посредством модулярного экспоненциатора.

Получатель платежа в данном примере действует также как и в примере 7.

Банк, убедившись, что в хранилище платежных счетов запись о платежном счете с открытым ключом подписи EP и проверив правильность подписи платежного сертификата sign открывает платежный счет, связанный с открытым ключом EP, кредитует его на сумму 116 рублей, в предположении, что стоимость операции открытия платежного счета 1 рубль, и проверив подпись платежного поручения плательщика PayerOrder открытым ключом подписи EP, проверив подпись платежного поручения продавца SellerOrder открытым ключом подписи счета No1, проверив совпадение условий платежа, содержащихся в платежных поручениях плательщика и продавца, заносит в информационное хранилище подписанное платежное поручение плательщика PayerOrder, производит дебетование платежного счета на сумму 115.5 рублей, кредитует на счет получателя платежа на сумму 114.5 рублей, в предположении, что стоимость проведения платежной операции банком равна 1 рублю, сохраняет подписанное поручение получателя платежа SellerOrder в своем информационном хранилище. После этого банк формирует квитанцию продавца, подтверждающую факт кредитования счета с номером No1 на сумму 114.5 рублей, подписывает ее и доставляет продавцу, который, проверив правильность подписи банка для полученной квитанции, считает платеж проведенным, и сообщает плательщику об успешном проведении платежа.

Оставшаяся на платежном сертификате сумма, равная разности 320 рублей и 117 рублей, может быть доставлена в банк и потрачена при других платежных операциях.

В качестве других частных случаев способа по второму варианту заявитель отмечает возможность реализации в виде многих иных комбинаций зависимых пунктов 16-29, а также возможность шифрования, дешифрования и перекодировки данных при их передаче по коммуникационным сетям, которые не меняют сущности заявленного изобретения.

Кроме того, оператор платежной системы при авторизации платежного сертификата может проверять подпись платежного сертификата как открытыми так и секретными денежными ключами. Помимо этого, при ошибках работы коммуникационных сетей при проведении вовлеченных в проведение платежа операций, такие операции могут быть повторены до их успешного завершения без ущерба для вовлеченных сторон.

Указанный выше технический результат при реализации изобретения достигается тем, что способ проведения платежей по третьему варианту, заключающийся в выборе оператором платежной системы денежных секретных ключей и соответствующих денежных открытых ключей посредством генератора ключей, выборе плательщиком посредством датчика случайных чисел по меньшей мере одной основы платежного сертификата, которая содержит номер платежного сертификата, являющийся одновременно и подписью нулевого уровня платежного сертификата, проведении по меньшей мере одной операции пополнения платежного устройства, при которой плательщик создает посредством датчика случайных чисел по меньшей мере одной

основу платежного сертификата, которая включает его номер, и формирует денежный запрос, включающий замаскированный номер созданной основы платежного сертификата в качестве данных для изготовления вслепую денежной подписи, и доставляют его посредством коммуникационных сетей в платежный сервер оператора платежной системы, который по полученному денежному запросу определяет источник и сумму кредитования, создает при изготовлении вслепую денежной подписи данные для демаскировки посредством введения содержащихся в запросе данных для изготовления вслепую денежной подписи и соответствующего сумме кредитования денежного секретного ключа в подписывающее устройство и доставляет посредством коммуникационных сетей созданные данные для демаскировки в платежное устройство плательщика, после чего осуществляют проверку правильности доставленных данных для демаскировки посредством их обработки денежным открытым ключом, соответствующим использованному оператором денежному секретному ключу, и принимает их в качестве данных для получения подписи платежного сертификата, проведении по меньшей мере одной операции авторизации оператором платежной системы платежного сертификата, подпись которого доставляют посредством коммуникационных сетей в платежный сервер оператора платежной системы, который осуществляет проверку правильности доставленной подписи платежного сертификата введением ее в устройство для проверки подписи, проведении по меньшей мере одной операции открытия у оператора платежной системы счета получателя платежа, проведении плательщиком по меньшей мере одной платежной операции, при которой подпись и основу используемого при платеже платежного сертификата включают в платежные данные, доставляемые получателю платежа, который формирует свое платежное поручение, включающее полученные от плательщика подпись и основу платежного сертификата, и доставляет его посредством коммуникационных сетей в платежный сервер оператора платежной системы, который по платежеспособности используемого при платеже платежного сертификата осуществляет кредитование счета получателя платежа на основе его платежного поручения, формирует свой ответ на платежное поручение получателя платежа и доставляет его получателю платежа, который по ответу оператора платежной системы судит о проведении платежа, *отличается тем, что* в основу платежного сертификата дополнительно включают идентификатор открытого ключа подписи платежного сертификата, предварительно изготовленного совместно с соответствующим ему секретным ключом подписи посредством генератора ключей, причем открытый ключ подписи платежного сертификата доставляют посредством коммуникационных сетей в платежный сервер оператора платежной системы, который при проведении операции авторизации дополнительно осуществляет поиск платежного счета, связанного с авторизуемым им платежном сертификатом, и в случае отсутствия такого счета, открывает его, а при наличии такого счета производит его кредитование на основе уровней авторизованных платежных сертификатов, связанных с данным счетом, доставляемую оператору платежной системы подпись авторизуемого им платежного сертификата плательщик изготавливает по соответствующим этому платежному сертификату данным для получения посредством демаскировки подписи платежного сертификата, причем уровень изготавливаемой подписи выбирают произвольно в пределах уровня секретного ключа, использованного для изготовления данных для получения посредством демаскировки подписи платежного сертификата, дополнительно по меньшей мере один из плательщиков проводит по меньшей мере одну операцию пополнения платежного устройства посредством операции пополнения платежного сертификата, при которой выбирают платежный сертификат и формируют денежный запрос, включающий данные для изготовления вслепую денежной подписи, в качестве которых берут замаскированную подпись платежного сертификата наибольшего

уровня, предварительно изготовленную посредством демаскировки данных для получения подписи платежного сертификата, и доставляют его в платежный сервер оператора платежной системы, который по полученному денежному запросу определяет источник и сумму кредитования по денежному запросу, создает при изготовлении вслепую денежной подписи данные для демаскировки посредством обработки содержащихся в запросе данных для изготовления вслепую денежной подписи соответствующим сумме кредитования денежным секретным ключом и доставляет их отправителю денежного запроса, который осуществляет проверку правильности доставленных ему данных для демаскировки посредством их обработки денежным открытым ключом, соответствующим использованному оператором денежному секретному ключу, и принимает их в качестве данных для получения подписи платежного сертификата, в платежные данные дополнительно включают платежное поручение плательщика и подпись для этого платежного поручения, которую предварительно получают на выходе подписывающего устройства после введения в него платежного поручения и секретного ключа подписи используемого платежного сертификата, причем в платежное поручение включают сведения о получателе платежа, условия платежа и идентификатор используемого платежного сертификата, при проведении по меньшей мере одной операции открытия у оператора платежной системы счета получателя платежа дополнительно получатель платежа выбирает посредством датчика случайных чисел секретный ключ подписи счета и соответствующий открытый ключ подписи счета, причем открытый ключ подписи счета доставляют посредством коммуникационных сетей в платежный сервер оператора платежной системы, который связывает его с открываемым счетом, при формировании платежного поручения получателя платежа в него включают условия платежа, изготавливают подпись платежного поручения получателя платежа посредством обработки его секретным ключом подписи счета получателя платежа, а изготовленную подпись доставляют посредством коммуникационных сетей в платежный сервер оператора платежной системы, при проведении платежной операции оператор платежной системы дополнительно включает в свой ответ на платежное поручение получателя платежа квитанцию получателя платежа, предварительно подписанную посредством введения ее и одного из секретных ключей подписи оператора платежной системы в подписывающее устройство, до кредитования получателя платежа дополнительно проверяют правильность подписи для платежного поручения плательщика посредством устройства для проверки подписи, в которое предварительно вводят платежное поручение и открытый ключ подписи используемого платежного сертификата, проверяют правильность подписи для платежного поручения получателя платежа посредством устройства для проверки подписи, в которое предварительно вводят платежное поручение получателя платежа и открытый ключ подписи счета получателя платежа, контролируют соответствие условий платежа, содержащихся в платежных поручениях, при кредитовании счета получателя платежа дополнительно осуществляют дебетование платежного счета, связанного с используемым при платеже платежным сертификатом, получатель платежа по полученному ответу оператора платежной системы на свое платежное поручение осуществляет проверку правильности подписи для квитанции получателя платежа посредством введения ее и открытого ключа подписи, соответствующего использованному секретному ключу подписи оператора платежной системы в устройство для проверки подписи, по выходу которого судит о проведении платежа, и доставляет плательщику данные, по которым плательщик судит о проведении платежа.

Указанный выше технический результат в частных случаях конкретной реализации может достигаться, кроме того, тем, что при выборе основы платежного сертификата в

нее включают дополнительный номер, а проверку действительности основы платежного сертификата при проверке правильности доставленной подписи платежного сертификата осуществляют по совпадению номера платежного сертификате и преобразованного посредством вычислителя наперед заданной односторонней функции дополнительного номера, причем выбор посредством датчика случайных чисел основы платежного сертификата, удовлетворяющей выбранному критерию действительности основ платежных сертификатов, осуществляют посредством выбора односторонней функции, выбором посредством датчика случайных чисел дополнительного номера, а номер получают посредством обработки выбранного дополнительного номера выбранной односторонней функцией.

Кроме того, при включении основу платежного сертификата идентификатора открытого ключа подписи платежного сертификата, в качестве этого идентификатора используют сам открытый ключ подписи платежного сертификата.

В частности, при включении в основу платежного сертификата идентификатор открытого ключа подписи платежного сертификата включают в основу в качестве дополнительного номера.

Помимо этого, перед включением в платежные данные платежного поручение плательщика осуществляют его шифрование одним из открытых ключей для шифрования оператора платежной системы, а оператор платежной системы производит дешифрование полученного от получателя платежа платежного поручения плательщика секретным ключом оператора платежной системы, соответствующим использованному плательщиком открытому ключу для шифрования.

Более того, оператор платежной системы осуществляет шифрование своего ответа на платежное поручение получателя платежа.

Помимо этого, в условия платежа, содержащиеся в платежном поручении плательщика, включают данные обязательства получателя платежа перед плательщиком.

В частности, при подготовке плательщиком платежных данных производят обработку данных обязательства получателя платежа перед плательщиком наперед заданной маскирующей функцией, а данные, полученные при этой обработке, включают в подготавливаемое платежное поручение плательщика, получатель платежа производит обработку данных обязательства получателя платежа перед плательщиком наперед заданной маскирующей функцией, а данные, полученные при этой обработке, включают в платежное поручение получателя платежа.

Кроме того, наперед заданную маскирующую функцию выбирают произвольно из множества односторонних функций.

Более того, получатель платежа подписывает данные обязательства получателя платежа перед плательщиком одним из своих секретных ключей для подписи, получатель платежа до платежной операции проверяет подпись получателя для данных обязательства получателя платежа перед плательщиком.

В частности, при проведении по меньшей мере одной операции пополнения платежного устройства в качестве источника кредитования используют счет плательщика, который предварительно кредитуют при по меньшей мере одной платежной операции.

Помимо этого, при проведении по меньшей мере одной операции пополнения платежного устройства в качестве источника кредитования используют банковскую карточку.

Более того, при открытии платежного счета, связанного с авторизуемым платежном сертификатом, производят его предварительное дебетование.

В частности, при операции пополнения платежного сертификата формирование денежного запроса производят в соответствии с единой для всех денежных запросов

структурой.

Помимо этого, подпись авторизуемого платежного сертификата изготавливают посредством понижения уровня имеющейся у плательщика подписи платежного сертификата.

В частности, при проведении платежной операции в качестве плательщика выступает получатель платежа.

Более того, оператора платежной системы может иметь по меньшей мере два платежных сервера.

Сущность способа проведения платежей по третьему варианту состоит в том же, что и по второму варианту, за исключением того, что плательщику дополнительно доступна операция пополнения своего платежного устройства за счет пополнения уже имеющихся у него платежных сертификатов путем увеличения уровня их подписи с помощью оператора платежной системы, изготавливающего вслепую подпись платежного сертификата повышенного уровня. При этом оператор платежной системы не имеет возможности определить, служит ли изготавливаемые им в ходе изготовления вслепую денежной подписи данные для демаскировки для пополнения уже имеющегося платежного сертификата, или они служат для наполнения вновь созданного платежного сертификата. При этом при пополнении одного и того же платежного сертификата плательщик может использовать различные источники кредитования, не связывая их между собой.

Единая совокупность признаков третьего варианта заявленного способа, перечисленных выше, связана причинно-следственной связью с ранее изложенным техническим результатом изобретения, заключающемся в том, что при проведении платежей по открытым телекоммуникационным сетям денежные интересы каждого участника защищены от злоупотреблений всех других участников, причем плательщики и получатели платежей имееют возможность защиты своей приватности. Помимо этого доступны платежи в диапазоне от микроплатежей до платежей бизнес-уровня, время проведения платежа зависит только от быстроты действия сетевых соединений, но не от суммы платежа, число клиентов, которые могут быть обслужены оператором платежной системы, растет пропорционально его ресурсам.

Указанный выше технический результат при осуществлении способа проведения платежей по третьему варианту достигается, в частности, тем, что плательщик защищен от нечестного оператора платежной системы тем, что последний обязан отчитываться о проведенных им расходах по платежному сертификату подписанным платежным поручением плательщика, приватность плательщика защищена процедурой изготовления подписи платежного сертификата вслепую, а приватность получателя платежа может быть защищена тем, что при открытии счета получатель платежа не обязан сообщать никаких сведений, позволяющих определить его личность. Диапазон платежей и независимость времени проведения платежей обеспечены независимость суммы платежа от номинальных стоимостей, соответствующих денежным ключам. Рост числа клиентов пропорционально ресурсам оператора платежной системы обеспечен тем, что с помощью одного платежного сертификата можно проводить большое число платежей, а число используемых платежных сертификатов может быть ограничено стоимостью операции открытия платежного счета и операции изготовления вслепую денежной подписи.

Ниже заявитель приводит пример конкретной реализации способа проведения платежей по третьему варианту.

Пример 10

В этом примере используются обозначения и соглашения, принятые в примере 9.

Банк, плательщик и продавец действуют также как и в примере 9, за исключением того, что плательщик в некоторый момент времени после получения им подписи SIGN платежного сертификата уровня (M1, M2, M3) = (20, 3, 0), что соответствует сумме 320 рублей, принимает решение пополнить этот платежный сертификат на 190 рублей. Для этого плательщик формирует денежный запрос в банк точно также как и в примере 4, за исключением того, что вместо маскировки номера X он маскирует имеющуюся у него подпись платежного сертификата SIGN в соответствии с открытой экспонентой, определенной уровнем (U1,U2,U3), где U1= 90, U2=1, U3=0 удовлетворяют соотношению 190 = U1×S1 + U2×S2 +U3×S3 и получает замаскированные данные X', которые доставляет в банк вместе с указанием, возможно иного, источника кредитования и суммой кредитования 190 рублей в качестве денежного запроса.

Далее, банк действует как и в примере 4, выбирает секретный денежный ключ, соответствующий сумме кредитования в 190 рублей, изготавливает данные для демаскировки SIGN'. Получив данные для демаскировки SIGN' плательщик изготавливает новую подпись платежного сертификата SIGN уровня (M1 + U1, M2 + U2, M3 + U3) = (110, 4, 0) демаскировкой полученных данных SIGN' и получает тем самым годный для проведения платежной операции платежный сертификат номинальной стоимостью 510 рублей.

В качестве других частных случаев способа по третьему варианту заявитель отмечает возможность реализации в виде многих иных комбинаций зависимых пунктов 31-46, а также возможность шифрования, дешифрования и перекодировки данных при их передаче по коммуникационным сетям, которые не меняют сущности заявленного изобретения.

Кроме того, оператор платежной системы при авторизации платежного сертификата может проверять подпись платежного сертификата как открытыми так и секретными денежными ключами. Помимо этого, при ошибках работы коммуникационных сетей при проведении вовлеченных в проведение платежа операций, такие операции могут быть повторены до их успешного завершения без ущерба для вовлеченных сторон.

Указанный выше технический результат при реализации изобретения достигается тем, что способ проведения платежей по четвертому варианту, заключающийся в выборе оператором платежной системы денежных секретных ключей и соответствующих денежных открытых ключей посредством генератора ключей, выборе плательщиком посредством датчика случайных чисел по меньшей мере одной основы платежного сертификата, которая содержит номер платежного сертификата, являющийся одновременно и подписью нулевого уровня платежного сертификата, проведении по меньшей мере одной операции пополнения платежного устройства, при которой плательщик создает посредством датчика случайных чисел по меньшей мере одной основу платежного сертификата, которая включает его номер, и формирует денежный запрос, включающий замаскированный номер созданной основы платежного сертификата в качестве данных для изготовления вслепую денежной подписи, и доставляют его посредством коммуникационных сетей в платежный сервер оператора платежной системы, который по полученному денежному запросу определяет источник и сумму кредитования, создает при изготовлении вслепую денежной подписи данные для демаскировки посредством введения содержащихся в запросе данных для изготовления вслепую денежной подписи и соответствующего сумме кредитования денежного секретного ключа в подписывающее устройство и доставляет посредством коммуникационных сетей созданные данные для демаскировки в платежное устройство плательщика, после чего изготавливают подпись платежного сертификата введением доставленных данных для демаскировки в демаскирующее устройство и осуществляют проверку правильности изготовленной подписи платежного сертификата введением ее

и денежного открытого ключа, соответствующего использованному оператором денежному секретному ключу, в устройство для проверки подписи, проведении по меньшей мере одной операции авторизации оператором платежной системы платежного сертификата, подпись которого плательщик доставляет посредством коммуникационных сетей в платежный сервер оператора платежной системы, который осуществляет проверку правильности доставленной подписи платежного сертификата введением ее в устройство для проверки подписи, проведении по меньшей мере одной операции открытия у оператора платежной системы счета получателя платежа, проведении плательщиком по меньшей мере одной платежной операции, при которой подпись и основу используемого при платеже платежного сертификата включают в платежные данные, доставляемые получателю платежа, который формирует свое платежное поручение, включающее полученные от плательщика подпись и основу платежного сертификата, и доставляет его посредством коммуникационных сетей в платежный сервер оператора платежной системы, который по платежеспособности используемого при платеже платежного сертификата осуществляет кредитование счета получателя платежа на основе его платежного поручения, формирует свой ответ на платежное поручение получателя платежа и доставляет его получателю платежа, который по ответу оператора платежной системы судит о проведении платежа, *отличается тем, что* в основу платежного сертификата дополнительно включают идентификатор открытого ключа подписи платежного сертификата, предварительно изготовленного совместно с соответствующим ему секретным ключом подписи посредством генератора ключей, причем открытый ключ подписи платежного сертификата доставляют посредством коммуникационных сетей в платежный сервер оператора платежной системы, который при проведении операции авторизации дополнительно осуществляет поиск платежного счета, связанного с авторизуемым им платежном сертификатом, и в случае отсутствия такого счета, открывает его, а при наличии такого счета производит его кредитование на основе уровней авторизованных платежных сертификатов, связанных с данным счетом, дополнительно по меньшей мере один из плательщиков проводит по меньшей мере одну операцию перевода с одного из платежных сертификатов на другой, один из которых выбирают в качестве исходного платежного сертификата, а другой в качестве целевого платежного сертификата, формируют денежный запрос, включающий данные для изготовления вслепую денежной подписи, в качестве которых берут предварительно изготовленную замаскированную подпись целевого платежного сертификата наибольшего уровня, и платежное поручение плательщика с подписью, которую предварительно получают на выходе подписывающего устройства после введения в него платежного поручения плательщика и секретного ключа подписи исходного платежного сертификата, причем в платежное поручение плательщика включают идентификатор исходного платежного сертификата и сумму перевода, денежный запрос доставляют посредством коммуникационных сетей в платежный сервер оператора платежной системы, который проверяет правильность подписи для платежного поручения плательщика посредством устройства для проверки подписи, в которое предварительно вводят платежное поручение плательщика и открытый ключ подписи исходного платежного сертификата, осуществляют кредитование целевого платежного сертификата, при котором производят дебетование платежного счета, связанного с исходным платежным сертификатом, создают при изготовлении вслепую денежной подписи данные для демаскировки посредством обработки содержащихся в денежном запросе данных для изготовления вслепую денежной подписи денежным секретным ключом, соответствующим сумме кредитования целевого платежного сертификата, и доставляют их плательщику, который осуществляет проверку правильности доставленных ему данных для демаскировки посредством их обработки денежным

открытым ключом, соответствующим использованному оператором платежной системы денежному секретному ключу, и принимает их в качестве данных для получения подписи целевого платежного сертификата, доставляемую оператору платежной системы подпись авторизуемого им платежного сертификата плательщик изготавливает по соответствующим этому платежному сертификату данным для получения посредством демаскировки подписи платежного сертификата, причем уровень изготавливаемой подписи выбирают произвольно в пределах уровня секретного ключа, использованного для изготовления данных для получения посредством демаскировки подписи платежного сертификата, в платежные данные дополнительно включают платежное поручение плательщика с подписью, которую предварительно получают на выходе подписывающего устройства после введения в него платежного поручения плательщика и секретного ключа подписи используемого платежного сертификата, причем в платежное поручение плательщика включают сведения о получателе платежа, условия платежа и идентификатор используемого платежного сертификата, при проведении по меньшей мере одной операции открытия у оператора платежной системы счета получателя платежа дополнительно получатель платежа выбирает посредством датчика случайных чисел секретный ключ подписи счета и соответствующий открытый ключ подписи счета, причем открытый ключ подписи счета доставляют посредством коммуникационных сетей в платежный сервер оператора платежной системы, который связывает его с открываемым счетом, при формировании платежного поручения получателя платежа в него включают условия платежа, изготавливают подпись платежного поручения получателя платежа посредством обработки его секретным ключом подписи счета получателя платежа, а изготовленную подпись доставляют посредством коммуникационных сетей в платежный сервер оператора платежной системы, при проведении платежной операции оператор платежной системы дополнительно включает в свой ответ на платежное поручение получателя платежа квитанцию получателя платежа, предварительно подписанную посредством введения ее и одного из секретных ключей подписи оператора платежной системы в подписывающее устройство, до кредитования получателя платежа дополнительно проверяют правильность подписи для платежного поручения плательщика посредством устройства для проверки подписи, в которое предварительно вводят платежное поручение плательщика и открытый ключ подписи используемого платежного сертификата, проверяют правильность подписи для платежного поручения получателя платежа посредством устройства для проверки подписи, в которое предварительно вводят платежное поручение получателя платежа и открытый ключ подписи счета получателя платежа, контролируют соответствие условий платежа, содержащихся в платежных поручениях плательщика и получателя платежа, при кредитовании счета получателя платежа дополнительно осуществляют дебетование платежного счета, связанного с используемым при платеже платежным сертификатом, получатель платежа по полученному ответу оператора платежной системы на свое платежное поручение осуществляет проверку правильности подписи для квитанции получателя платежа посредством введения ее и открытого ключа подписи, соответствующего использованному секретному ключу подписи оператора платежной системы в устройство для проверки подписи, по выходу которого судит о проведении платежа, и доставляет плательщику данные, по которым плательщик судит о проведении платежа.

Указанный выше технический результат в частных случаях конкретной реализации может достигаться, кроме того, тем, что при выборе основы платежного сертификата в нее включают дополнительный номер, а проверку действительности основы платежного сертификата при проверке правильности доставленной подписи платежного сертификата осуществляют по совпадению номера платежного

сертификате и преобразованного посредством вычислителя наперед заданной односторонней функции дополнительного номера, причем выбор посредством датчика случайных чисел основы платежного сертификата, удовлетворяющей выбранному критерию действительности основ платежных сертификатов, осуществляют посредством выбора односторонней функции, выбором посредством датчика случайных чисел дополнительного номера, а номер получают посредством обработки выбранного дополнительного номера выбранной односторонней функцией.

Кроме того, при включении основу платежного сертификата идентификатора открытого ключа подписи платежного сертификата, в качестве этого идентификатора используют сам открытый ключ подписи платежного сертификата.

В частности, при включении в основу платежного сертификата идентификатор открытого ключа подписи платежного сертификата включают в основу в качестве дополнительного номера.

Помимо этого, перед включением в платежные данные платежного поручение плательщика осуществляют его шифрование одним из открытых ключей для шифрования оператора платежной системы, а оператор платежной системы производит дешифрование полученного от получателя платежа платежного поручения плательщика секретным ключом оператора платежной системы, соответствующим использованному плательщиком открытому ключу для шифрования.

Более того, оператор платежной системы осуществляет шифрование своего ответа на платежное поручение получателя платежа.

В частности, в условия платежа, содержащиеся в платежном поручении плательщика, включают данные обязательства получателя платежа перед плательщиком.

Кроме того, при подготовке плательщиком платежных данных производят обработку данных обязательства получателя платежа перед плательщиком наперед заданной маскирующей функцией, а данные, полученные при этой обработке, включают в подготавливаемое платежное поручение плательщика, получатель платежа производит обработку данных обязательства получателя платежа перед плательщиком наперед заданной маскирующей функцией, а данные, полученные при этой обработке, включают в платежное поручение получателя платежа.

В частности, наперед заданную маскирующую функцию выбирают произвольно из множества односторонних функций.

Помимо этого, получатель платежа подписывает данные обязательства получателя платежа перед плательщиком одним из своих секретных ключей для подписи, получатель платежа до платежной операции проверяет подпись получателя для данных обязательства получателя платежа перед плательщиком.

В частности, при проведении по меньшей мере одной операции пополнения платежного устройства в качестве источника кредитования используют счет плательщика, который предварительно кредитуют при по меньшей мере одной платежной операции.

Кроме того, при проведении по меньшей мере одной операции пополнения платежного устройства в качестве источника кредитования используют банковскую карточку.

Помимо этого, при открытии платежного счета, связанного с авторизуемым платежном сертификатом, производят его предварительное дебетование.

Более того, при операции пополнения платежного сертификата формирование денежного запроса производят в соответствии с единой для всех денежных запросов структурой.

В частности, подпись авторизуемого платежного сертификата изготавливают посредством понижения уровня имеющейся у плательщика подписи платежного

сертификата.

Кроме того, при проведении платежной операции в качестве плательщика выступает получатель платежа.

Более того, оператор платежной системы может иметь по меньшей мере два платежных сервера.

Сущность способа проведения платежей по четвертому варианту состоит в том же, что и по третьему варианту, за исключением того, что плательщику дополнительно доступна операция перевода с одного своего платежного сертификата на другой. При этом данный перевод производится посредством изготовления вслепую подписи целевого платежного сертификата, то есть того платежного сертификата, номинальная стоимость которого увеличивается при этой операции. Кредитование целевого платежного сертификата происходит за счет платежного счета, связанного с исходным платежным сертификатом.

Единая совокупность признаков четвертого варианта заявленного способа, перечисленных выше, связана причинно-следственной связью с ранее изложенным техническим результатом изобретения, заключающемся в том, что при проведении платежей по открытым телекоммуникационным сетям денежные интересы каждого участника защищены от злоупотреблений всех других участников, причем плательщики и получатели платежей имеют возможность защиты своей приватности. Помимо этого доступны платежи в диапазоне от микроплатежей до платежей бизнес-уровня, время проведения платежа зависит только от быстроты действия сетевых соединений, но не от суммы платежа, число клиентов, которые могут быть обслужены оператором платежной системы, растет пропорционально его ресурсам.

Указанный выше технический результат при осуществлении способа проведения платежей по четвертому варианту достигается, в частности, тем, что плательщик защищен от нечестного оператора платежной системы тем, что последний обязан отчитываться о проведенных им расходах по платежному сертификату подписанным платежным поручением плательщика, приватность плательщика защищена процедурой изготовления подписи платежного сертификата вслепую, а приватность получателя платежа может быть защищена тем, что при открытии счета получатель платежа не обязан сообщать никаких сведений, позволяющих определить его личность. Диапазон платежей и независимость времени проведения платежей обеспечены независимость суммы платежа от номинальных стоимостей, соответствующих денежным ключам. Рост числа клиентов пропорционально ресурсам оператора платежной системы обеспечен тем, что с помощью одного платежного сертификата можно проводить большое число платежей, а число используемых платежных сертификатов может быть ограничено стоимостью операции открытия платежного счета и операции изготовления вслепую денежной подписи.

Ниже заявитель приводит пример конкретной реализации способа проведения платежей по четвертому варианту.

Пример 11

В этом примере используются обозначения и соглашения, принятые в примере 10. Банк, плательщик и продавец действуют также как и в примере 10, за исключением того, что плательщик как в примере 4 или как в примере 10 получает платежный сертификат, который принимает за целевой. После этого плательщик пополняет целевой платежный сертификат как и в примере 10, за исключением того, что в качестве источника кредитования указывает платежный счет, связанный с исходным платежным сертификатом. Конечно, платежное поручение банку должно быть подписано секретным ключом подписи исходного платежного сертификата, а банк должен сохранить это подписанное поручение.

В качестве других частных случаев способа по четвертому варианту заявитель отмечает возможность реализации в виде многих иных комбинаций зависимых пунктов 48-63, а также возможность шифрования, дешифрования и перекодировки данных при их передаче по коммуникационным сетям, которые не меняют сущности заявленного изобретения.

Кроме того, оператор платежной системы при авторизации платежного сертификата может проверять подпись платежного сертификата как открытыми так и секретными денежными ключами. Помимо этого, при ошибках работы коммуникационных сетей при проведении вовлеченных в проведение платежа операций, такие операции могут быть повторены до их успешного завершения без ущерба для вовлеченных сторон.

Помимо этого при переводе с одного платежного сертификата на другой можно использовать предложенный в [8] способ получения "слепой сдачи" для получения остатка исходного платежного сертификата, размер которого будет скрыт от оператора платежной системы.

Указанный выше технический результат при реализации изобретения достигается тем, что способ проведения платежей по пятому варианту, заключающийся в выборе оператором платежной системы денежных секретных ключей и соответствующих денежных открытых ключей посредством генератора ключей, проведении по меньшей мере одной операции пополнения платежного устройства, при которой плательщик создает посредством датчика случайных чисел по меньшей мере одной основу платежного сертификата, которая включает его номер, и получает подпись платежного сертификата посредством изготовления вслепую денежной подписи оператором платежной системы, проведении плательщиком по меньшей мере одной платежной операции, при которой подпись и основу используемого при платеже платежного сертификата включают в платежные данные, доставляемые получателю платежа, который формирует свое платежное поручение, включающее полученные от плательщика подпись и основу платежного сертификата, и доставляет его посредством коммуникационных сетей в платежный сервер оператора платежной системы, который по платежеспособности используемого при платеже платежного сертификата осуществляет кредитование счета получателя платежа на основе его платежного поручения, причем при проверке платежеспособности используемого при платеже платежного сертификата оператор платежной системы проводит операцию его авторизации, при которой по наличию информации об авторизуемом платежном сертификате в информационном хранилище отказывают в авторизации, а по ее отсутствию осуществляют проверку правильности доставленной подписи платежного сертификата введением ее в устройство для проверки подписи, и в случае правильности заносят информацию об авторизуемом платежном сертификате в информационное хранилище, после чего формируют ответ оператора платежной системы на платежное поручение получателя платежа и доставляют его получателю платежа, который по ответу оператора платежной системы судит о проведении платежа, *отличается тем, что* в основу платежного сертификата дополнительно включают идентификатор открытого ключа подписи платежного сертификата, предварительно изготовленного совместно с соответствующим ему секретным ключом подписи посредством генератора ключей, причем открытый ключ подписи платежного сертификата доставляют посредством коммуникационных сетей в платежный сервер оператора платежной системы, в платежные данные дополнительно включают платежное поручение плательщика с подписью, которую предварительно получают на выходе подписывающего устройства после введения в него платежного поручения плательщика и секретного ключа подписи используемого платежного сертификата, причем в платежное поручение плательщика включают

сведения о получателе платежа, условия платежа и идентификатор используемого платежного сертификата, при проведении операции пополнения платежного устройства плательщик дополнительно формирует платежное требование, включающее замаскированную подпись выбранного платежного сертификата в качестве данных для изготовления вслепую денежной подписи, и подписанное одним из секретных ключей подписи плательщика, и доставляет его промежуточному плательщику, который проверяет подпись для платежного требования открытым ключом подписи плательщика, соответствующим использованному секретному ключу подписи плательщика, формирует и доставляет в платежный сервер оператора платежной системы денежный запрос, который включает дополнительно замаскированную промежуточным плательщиком полученную от плательщика замаскированную подпись выбранного платежного сертификата и идентификатор счета промежуточного плательщика, причем денежный запрос подписывают секретным ключом счета промежуточного плательщика, а оператор платежной системы проверяет подпись денежного запроса промежуточного плательщика открытым ключом счета, идентификатор которого содержится в денежном запросе, осуществляет дебетование этого счета, создает при изготовлении вслепую денежной подписи данные для демаскировки, которые доставляют промежуточному плательщику, который осуществляет проверку правильности доставленных ему данных для демаскировки посредством их обработки денежным открытым ключом, соответствующим использованному оператором платежной системы денежному секретному ключу, производит их демаскировку, результат которой доставляют плательщику, который изготавливает подпись платежного сертификата демаскировкой полученных от промежуточного плательщика данных для демаскировки, при проведении по меньшей мере одной операции открытия у оператора платежной системы счета получателя платежа дополнительно получатель платежа выбирает посредством датчика случайных чисел секретный ключ подписи счета и соответствующий открытый ключ подписи счета, причем открытый ключ подписи счета доставляют посредством коммуникационных сетей в платежный сервер оператора платежной системы, который связывает его с открываемым счетом, при формировании платежного поручения получателя платежа в него включают условия платежа, изготавливают подпись платежного поручения получателя платежа посредством обработки его секретным ключом подписи счета получателя платежа, а изготовленную подпись доставляют посредством коммуникационных сетей в платежный сервер оператора платежной системы, при проведении платежной операции оператор платежной системы дополнительно включает в свой ответ на платежное поручение получателя платежа квитанцию получателя платежа, предварительно подписанную посредством введения ее и одного из секретных ключей подписи оператора платежной системы в подписывающее устройство, до кредитования получателя платежа дополнительно проверяют правильность подписи для платежного поручения плательщика посредством устройства для проверки подписи, в которое предварительно вводят платежное поручение плательщика и открытый ключ подписи используемого платежного сертификата, в информационное хранилище при авторизации платежного сертификата заносят подписанное платежное поручение плательщика, проверяют правильность подписи для платежного поручения получателя платежа посредством устройства для проверки подписи, в которое предварительно вводят платежное поручение получателя платежа и открытый ключ подписи счета получателя платежа, контролируют соответствие условий платежа, содержащихся в платежных поручениях плательщика и получателя платежа, получатель платежа по полученному ответу оператора платежной системы на свое платежное поручение осуществляет проверку правильности подписи для квитанции получателя платежа посредством введения ее и открытого ключа

подписи, соответствующего использованному секретному ключу подписи оператора платежной системы в устройство для проверки подписи, по выходу которого судит о проведении платежа, и доставляет плательщику данные, по которым плательщик судит о проведении платежа.

Указанный выше технический результат в частных случаях конкретной реализации может достигаться, кроме того, тем, что при выборе при выборе основы платежного сертификата в нее включают дополнительный номер, а проверку действительности основы платежного сертификата при проверке правильности доставленной подписи платежного сертификата осуществляют по совпадению номера платежного сертификате и преобразованного посредством вычислителя наперед заданной односторонней функции дополнительного номера, причем выбор посредством датчика случайных чисел основы платежного сертификата, удовлетворяющей выбранному критерию действительности основ платежных сертификатов, осуществляют посредством выбора односторонней функции, выбором посредством датчика случайных чисел дополнительного номера, а номер получают посредством обработки выбранного дополнительного номера выбранной односторонней функцией.

Кроме того, при включении основу платежного сертификата идентификатора открытого ключа подписи платежного сертификата, в качестве этого идентификатора используют сам открытый ключ подписи платежного сертификата.

В частности, при включении в основу платежного сертификата идентификатор открытого ключа подписи платежного сертификата включают в основу в качестве дополнительного номера.

Помимо этого, перед включением в платежные данные платежного поручение плательщика осуществляют его шифрование одним из открытых ключей для шифрования оператора платежной системы, а оператор платежной системы производит дешифрование полученного от получателя платежа платежного поручения плательщика секретным ключом оператора платежной системы, соответствующим использованному плательщиком открытому ключу для шифрования.

Более того, оператор платежной системы осуществляет шифрование своего ответа на платежное поручение получателя платежа.

Кроме того, в условия платежа, содержащиеся в платежном поручении плательщика, включают данные обязательства получателя платежа перед плательщиком.

Помимо этого, при подготовке плательщиком платежных данных производят обработку данных обязательства получателя платежа перед плательщиком наперед заданной маскирующей функцией, а данные, полученные при этой обработке, включают в подготавливаемое платежное поручение плательщика, получатель платежа производит обработку данных обязательства получателя платежа перед плательщиком наперед заданной маскирующей функцией, а данные, полученные при этой обработке, включают в платежное поручение получателя платежа.

В частности, наперед заданную маскирующую функцию выбирают произвольно из множества односторонних функций.

Кроме того, получатель платежа подписывает данные обязательства получателя платежа перед плательщиком одним из своих секретных ключей для подписи, получатель платежа до платежной операции проверяет подпись получателя для данных обязательства получателя платежа перед плательщиком.

В частности, при проведении по меньшей мере одной операции пополнения платежного устройства в качестве источника кредитования используют счет плательщика, который предварительно кредитуют при по меньшей мере одной платежной операции.

Помимо этого, при проведении по меньшей мере одной операции пополнения

платежного устройства в качестве источника кредитования используют банковскую карточку.

В частности, при проведении платежной операции в качестве плательщика выступает получатель платежа.

Более того, оператора платежной системы может иметь по меньшей мере два платежных сервера .

Сущность способа проведения платежей по пятому варианту состоит в том же, что и по первому варианту, за исключением того, что плательщику получает подпись платежного сертификата посредством промежуточного плательщика, который производит платеж со своего счета на платежный сертификат плательщика. При этом промежуточный плательщик применяет дополнительную маскировку и, соответственно демаскировку проходящих через него данных для денежной подписи.

Единая совокупность признаков пятого варианта заявленного способа, перечисленных выше, связана причинно-следственной связью с ранее изложенным техническим результатом изобретения, заключающемся в том, что при проведении платежей по открытым телекоммуникационным сетям денежные интересы каждого участника защищены от злоупотреблений всех других участников, причем плательщики и получатели платежей имеют возможность защиты своей приватности.

Указанный выше технический результат при осуществлении способа проведения платежей по пятому варианту достигается, в частности, тем, что плательщик защищен от нечестного оператора платежной системы тем, что последний обязан отчитываться о проведенных им расходах по платежному сертификату подписанным платежным поручением плательщика, приватность плательщика защищена процедурой изготовления подписи платежного сертификата вслепую, а приватность получателя платежа может быть защищена тем, что при открытии счета получатель платежа не обязан сообщать никаких сведений, позволяющих определить его личность.

Ниже заявитель приводит пример конкретной реализации способа проведения платежей по пятому варианту.

Пример 12

В этом примере используются обозначения и соглашения, принятые в примере 7. Банк, плательщик и продавец действуют также как и в примере 7, за исключением того, что плательщик доставляет замаскированные данные X' промежуточному плательщику, который производит их дополнительную маскировку и, соответственно, демаскировку полученных от банка данных для демаскировки точно так, как плательщик производит маскировку и демаскировку в примере 4.

В качестве других частных случаев способа по пятому варианту заявитель отмечает возможность реализации в виде многих иных комбинаций зависимых пунктов 65-77, а также возможность шифрования, дешифрования и перекодировки данных при их передаче по коммуникационным сетям, которые не меняют сущности заявленного изобретения.

Кроме того, оператор платежной системы при авторизации платежного сертификата может проверять подпись платежного сертификата как открытыми так и секретными денежными ключами. Помимо этого, при ошибках работы коммуникационных сетей при проведении вовлеченных в проведение платежа операций, такие операции могут быть повторены до их успешного завершения без ущерба для вовлеченных сторон.

Указанный выше технический результат при реализации изобретения достигается тем, что способ проведения платежей по шестому варианту, заключающийся в выборе оператором платежной системы денежных секретных ключей и соответствующих

денежных открытых ключей посредством генератора ключей, выборе плательщиком посредством датчика случайных чисел по меньшей мере одной основы платежного сертификата, которая содержит номер платежного сертификата, являющийся одновременно и подписью нулевого уровня платежного сертификата, проведении по меньшей мере одной операции пополнения платежного устройства, при которой плательщик получает подпись платежного сертификата посредством изготовления вслепую денежной подписи оператором платежной системы, проведении по меньшей мере одной операции авторизации оператором платежной системы платежного сертификата, подпись которого плательщик доставляет посредством коммуникационных сетей в платежный сервер оператора платежной системы, который осуществляет проверку правильности доставленной подписи платежного сертификата введением ее в устройство для проверки подписи, проведении по меньшей мере одной операции открытия у оператора платежной системы счета получателя платежа, проведении плательщиком по меньшей мере одной платежной операции, при которой подпись и основу используемого при платеже платежного сертификата включают в платежные данные, доставляемые получателю платежа, который формирует свое платежное поручение, включающее полученные от плательщика подпись и основу платежного сертификата, и доставляет его посредством коммуникационных сетей в платежный сервер оператора платежной системы, который по платежеспособности используемого при платеже платежного сертификата осуществляет кредитование счета получателя платежа на основе его платежного поручения, формирует свой ответ на платежное поручение получателя платежа и доставляет его получателю платежа, который по ответу оператора платежной системы судит о проведении платежа, *отличается тем, что* в основу платежного сертификата дополнительно включают идентификатор открытого ключа подписи платежного сертификата, предварительно изготовленного совместно с соответствующим ему секретным ключом подписи посредством генератора ключей, причем открытый ключ подписи платежного сертификата доставляют посредством коммуникационных сетей в платежный сервер оператора платежной системы, который при проведении операции авторизации дополнительно осуществляет поиск платежного счета, связанного с авторизуемым им платежном сертификатом, и в случае отсутствия такого счета, открывает его, а при наличии такого счета производит его кредитование на основе уровней авторизованных платежных сертификатов, связанных с данным счетом, доставляемую оператору платежной системы подпись авторизуемого им платежного сертификата плательщик изготавливает по соответствующим этому платежному сертификату данным для получения посредством демаскировки подписи платежного сертификата, причем уровень изготавливаемой подписи выбирают произвольно в пределах уровня секретного ключа, использованного для изготовления данных для получения посредством демаскировки подписи платежного сертификата, дополнительно по меньшей мере один из плательщиков проводит по меньшей мере одну операцию пополнения платежного устройства посредством перевода со счета промежуточного плательщика, при которой плательщик дополнительно формирует платежное требование, включающее замаскированную подпись выбранного платежного сертификата в качестве данных для изготовления вслепую денежной подписи, и подписанное одним из секретных ключей подписи плательщика, и доставляет его промежуточному плательщику, который проверяет подпись для платежного требования открытым ключом подписи плательщика, соответствующим использованному плательщиком секретному ключу подписи, формирует и доставляет в платежный сервер оператора платежной системы денежный запрос, который включает дополнительно замаскированную промежуточным плательщиком полученную от плательщика замаскированную подпись выбранного платежного сертификата и

идентификатор счета промежуточного плательщика, причем денежный запрос подписывают секретным ключом счета промежуточного плательщика, а оператор платежной системы проверяет подпись денежного запроса промежуточного плательщика открытым ключом счета, идентификатор которого содержится в денежном запросе, осуществляет дебетование этого счета, создает при изготовлении вслепую денежной подписи данные для демаскировки, которые доставляют промежуточному плательщику, который осуществляет проверку правильности доставленных ему данных для демаскировки посредством их обработки денежным открытым ключом, соответствующим использованному оператором денежному секретному ключу, производит их демаскировку, результат которой доставляют плательщику, который изготавливает подпись платежного сертификата демаскировкой полученных от промежуточного плательщика данных для демаскировки, в платежные данные дополнительно включают платежное поручение плательщика с подписью, которую предварительно получают на выходе подписывающего устройства после введения в него платежного поручения и секретного ключа подписи используемого платежного сертификата, причем в платежное поручение включают сведения о получателе платежа, условия платежа и идентификатор используемого платежного сертификата, при проведении по меньшей мере одной операции открытия у оператора платежной системы счета получателя платежа дополнительно получатель платежа выбирает посредством датчика случайных чисел секретный ключ подписи счета и соответствующий открытый ключ подписи счета, причем открытый ключ подписи счета доставляют посредством коммуникационных сетей в платежный сервер оператора платежной системы, который связывает его с открываемым счетом, при формировании платежного поручения получателя платежа в него включают условия платежа, изготавливают подпись платежного поручения получателя платежа посредством обработки его секретным ключом подписи счета получателя платежа, а изготовленную подпись доставляют посредством коммуникационных сетей в платежный сервер оператора платежной системы, при проведении платежной операции оператор платежной системы дополнительно включает в свой ответ на платежное поручение получателя платежа квитанцию получателя платежа, предварительно подписанную посредством введения ее и одного из секретных ключей подписи оператора платежной системы в подписывающее устройство, до кредитования получателя платежа дополнительно проверяют правильность подписи для платежного поручения плательщика посредством устройства для проверки подписи, в которое предварительно вводят платежное поручение плательщика и открытый ключ подписи используемого платежного сертификата, проверяют правильность подписи для платежного поручения получателя платежа посредством устройства для проверки подписи, в которое предварительно вводят платежное поручение получателя платежа и открытый ключ подписи счета получателя платежа, контролируют соответствие условий платежа, содержащихся в платежных поручениях плательщика и получателя платежа, при кредитовании счета получателя платежа дополнительно осуществляют дебетование платежного счета, связанного с используемым при платеже платежным сертификатом, получатель платежа по полученному ответу оператора платежной системы на свое платежное поручение осуществляет проверку правильности подписи для квитанции получателя платежа посредством введения ее и открытого ключа подписи, соответствующего использованному секретному ключу подписи оператора платежной системы в устройство для проверки подписи, по выходу которого судит о проведении платежа, и доставляет плательщику данные, по которым плательщик судит о проведении платежа.

Указанный выше технический результат в частных случаях конкретной реализации может достигаться, кроме того, тем, что при выборе основы платежного сертификата в

нее включают дополнительный номер, а проверку действительности основы платежного сертификата при проверке правильности доставленной подписи платежного сертификата осуществляют по совпадению номера платежного сертификате и преобразованного посредством вычислителя наперед заданной односторонней функции дополнительного номера, причем выбор посредством датчика случайных чисел основы платежного сертификата, удовлетворяющей выбранному критерию действительности основ платежных сертификатов, осуществляют посредством выбора односторонней функции, выбором посредством датчика случайных чисел дополнительного номера, а номер получают посредством обработки выбранного дополнительного номера выбранной односторонней функцией.

Более того, при включении основу платежного сертификата идентификатора открытого ключа подписи платежного сертификата, в качестве этого идентификатора используют сам открытый ключ подписи платежного сертификата.

В частности, при включении в основу платежного сертификата идентификатор открытого ключа подписи платежного сертификата включают в основу в качестве дополнительного номера.

Кроме этого, перед включением в платежные данные платежного поручение плательщика осуществляют его шифрование одним из открытых ключей для шифрования оператора платежной системы, а оператор платежной системы производит дешифрование полученного от получателя платежа платежного поручения плательщика секретным ключом оператора платежной системы, соответствующим использованному плательщиком открытому ключу для шифрования.

Помимо этого, оператор платежной системы осуществляет шифрование своего ответа на платежное поручение получателя платежа.

Более того, в условия платежа, содержащиеся в платежном поручении плательщика, включают данные обязательства получателя платежа перед плательщиком.

Кроме этого, при подготовке плательщиком платежных данных производят обработку данных обязательства получателя платежа перед плательщиком наперед заданной маскирующей функцией, а данные, полученные при этой обработке, включают в подготавливаемое платежное поручение плательщика, получатель платежа производит обработку данных обязательства получателя платежа перед плательщиком наперед заданной маскирующей функцией, а данные, полученные при этой обработке, включают в платежное поручение получателя платежа.

В частности, наперед заданную маскирующую функцию выбирают произвольно из множества односторонних функций.

Помимо этого, получатель платежа подписывает данные обязательства получателя платежа перед плательщиком одним из своих секретных ключей для подписи, получатель платежа до платежной операции проверяет подпись получателя для данных обязательства получателя платежа перед плательщиком.

Более того, при проведении по меньшей мере одной операции пополнения платежного устройства в качестве источника кредитования используют счет плательщика, который предварительно кредитуют при по меньшей мере одной платежной операции.

Кроме этого, при проведении по меньшей мере одной операции пополнения платежного устройства в качестве источника кредитования используют банковскую карточку.

Помимо этого, при открытии платежного счета, связанного с авторизуемым платежном сертификатом, производят его предварительное дебетование.

В частности, при проведении платежной операции в качестве плательщика выступает получатель платежа.

Более того, оператор платежной системы может иметь по меньшей мере два

платежных сервера.

Сущность способа проведения платежей по шестому варианту состоит в том же, что и по второму варианту, за исключением того, что плательщику получает подпись платежного сертификата посредством промежуточного плательщика, который производит платеж со своего счета на платежный сертификат плательщика. При этом промежуточный плательщик применяет дополнительную маскировку и, соответственно демаскировку проходящих через него данных для денежной подписи.

Единая совокупность признаков шестого варианта заявленного способа, перечисленных выше, связана причинно-следственной связью с ранее изложенным техническим результатом изобретения, заключающемся в том, что при проведении платежей по открытым телекоммуникационным сетям денежные интересы каждого участника защищены от злоупотреблений всех других участников, причем плательщики и получатели платежей имеют возможность защиты своей приватности. Помимо этого доступны платежи в диапазоне от микроплатежей до платежей бизнес-уровня, время проведения платежа зависит только от быстроты действия сетевых соединений, но не от суммы платежа, число клиентов, которые могут быть обслужены оператором платежной системы, растет пропорционально его ресурсам.

Указанный выше технический результат при осуществлении способа проведения платежей по шестому варианту достигается, в частности, тем, что плательщик защищен от нечестного оператора платежной системы тем, что последний обязан отчитываться о проведенных им расходах по платежному сертификату подписанным платежным поручением плательщика, приватность плательщика защищена процедурой изготовления подписи платежного сертификата вслепую, а приватность получателя платежа может быть защищена тем, что при открытии счета получатель платежа не обязан сообщать никаких сведений, позволяющих определить его личность. Диапазон платежей и независимость времени проведения платежей обеспечены независимость суммы платежа от номинальных стоимостей, соответствующих денежным ключам. Рост числа клиентов пропорционально ресурсам оператора платежной системы обеспечен тем, что с помощью одного платежного сертификата можно проводить большое число платежей, а число используемых платежных сертификатов может быть ограничено стоимостью операции открытия платежного счета и операции изготовления вслепую денежной подписи.

Ниже заявитель приводит пример конкретной реализации способа проведения платежей по шестому варианту.

Пример 13

В этом примере используются обозначения и соглашения, принятые в примере 10. Банк, плательщик и продавец действуют также как и в примере 10, за исключением того, что плательщик при пополнении своего платежного устройства доставляет замаскированные как и в примере 4 данные X' промежуточному плательщику, который производит их дополнительную маскировку и, соответственно, демаскировку полученных от банка данных для демаскировки точно так, как плательщик производит маскировку и демаскировку в примере 4.

В качестве других частных случаев способа по шестому варианту заявитель отмечает возможность реализации в виде многих иных комбинаций зависимых пунктов 79-92, а также возможность шифрования, дешифрования и перекодировки данных при их передаче по коммуникационным сетям, которые не меняют сущности заявленного изобретения.

Кроме того, оператор платежной системы при авторизации платежного сертификата может проверять подпись платежного сертификата как открытыми так и секретными

денежными ключами. Помимо этого, при ошибках работы коммуникационных сетей при проведении вовлеченных в проведение платежа операций, такие операции могут быть повторены до их успешного завершения без ущерба для вовлеченных сторон.

Указанный выше технический результат при реализации изобретения достигается тем, что способ проведения платежей по седьмому варианту, заключающийся в выборе оператором платежной системы денежных секретных ключей и соответствующих денежных открытых ключей посредством генератора ключей, выборе плательщиком посредством датчика случайных чисел по меньшей мере одной основы платежного сертификата, которая содержит номер платежного сертификата, являющийся одновременно и подписью нулевого уровня платежного сертификата, проведении по меньшей мере одной операции пополнения платежного устройства, при которой плательщик получает подпись платежного сертификата посредством изготовления вслепую денежной подписи оператором платежной системы, проведении по меньшей мере одной операции авторизации оператором платежной системы платежного сертификата, подпись которого плательщик доставляет посредством коммуникационных сетей в платежный сервер оператора платежной системы, который осуществляет проверку правильности доставленной подписи платежного сертификата введением ее в устройство для проверки подписи, проведении по меньшей мере одной операции открытия у оператора платежной системы счета получателя платежа, проведении плательщиком по меньшей мере одной платежной операции, при которой подпись и основу используемого при платеже платежного сертификата включают в платежные данные, доставляемые получателю платежа, который формирует свое платежное поручение, включающее полученные от плательщика подпись и основу платежного сертификата, и доставляет его посредством коммуникационных сетей в платежный сервер оператора платежной системы, который по платежеспособности используемого при платеже платежного сертификата осуществляет кредитование счета получателя платежа на основе его платежного поручения, формирует свой ответ на платежное поручение получателя платежа и доставляет его получателю платежа, который по ответу оператора платежной системы судит о проведении платежа, *отличается тем, что* в основу платежного сертификата дополнительно включают идентификатор открытого ключа подписи платежного сертификата, предварительно изготовленного совместно с соответствующим ему секретным ключом подписи посредством генератора ключей, причем открытый ключ подписи платежного сертификата доставляют посредством коммуникационных сетей в платежный сервер оператора платежной системы, который при проведении операции авторизации дополнительно осуществляет поиск платежного счета, связанного с авторизуемым им платежном сертификатом, и в случае отсутствия такого счета, открывает его, а при наличии такого счета производит его кредитование на основе уровней авторизованных платежных сертификатов, связанных с данным счетом, доставляемую оператору платежной системы подпись авторизуемого им платежного сертификата плательщик изготавливает по соответствующим этому платежному сертификату данным для получения посредством демаскировки подписи платежного сертификата, причем уровень изготавливаемой подписи выбирают произвольно в пределах уровня секретного ключа, использованного для изготовления данных для получения посредством демаскировки подписи платежного сертификата, дополнительно по меньшей мере один из плательщиков проводит по меньшей мере одну операцию пополнения платежного устройства посредством перевода со счета промежуточного плательщика, при которой плательщик дополнительно формирует платежное требование, включающее замаскированную подпись выбранного платежного

сертификата в качестве данных для изготовления вслепую денежной подписи, и подписанное одним из секретных ключей подписи плательщика, и доставляет его промежуточному плательщику, который проверяет подпись для платежного требования открытым ключом подписи плательщика, соответствующим использованному плательщиком секретному ключу подписи, формирует и доставляет в платежный сервер оператора платежной системы денежный запрос, который включает дополнительно замаскированную промежуточным плательщиком полученную от плательщика замаскированную подпись выбранного платежного сертификата и идентификатор счета промежуточного плательщика, причем денежный запрос подписывают секретным ключом счета промежуточного плательщика, а оператор платежной системы проверяет подпись денежного запроса промежуточного плательщика открытым ключом счета, идентификатор которого содержится в денежном запросе, осуществляет дебетование этого счета, создает при изготовлении вслепую денежной подписи данные для демаскировки, которые доставляют промежуточному плательщику, который осуществляет проверку правильности доставленных ему данных для демаскировки посредством их обработки денежным открытым ключом, соответствующим использованному оператором денежному секретному ключу, производит их демаскировку, результат которой доставляют плательщику, который изготавливает подпись платежного сертификата демаскировкой полученных от промежуточного плательщика данных для демаскировки, дополнительно по меньшей мере один из плательщиков проводит по меньшей мере одну операцию пополнения платежного устройства посредством операции пополнения платежного сертификата, при которой выбирают платежный сертификат и формируют денежный запрос, включающий данные для изготовления вслепую денежной подписи, в качестве которых берут замаскированную подпись платежного сертификата наибольшего уровня, предварительно изготовленную посредством демаскировки данных для получения подписи платежного сертификата, и доставляют его в платежный сервер оператора платежной системы, который по полученному денежному запросу определяет источник и сумму кредитования по денежному запросу, создает при изготовлении вслепую денежной подписи данные для демаскировки посредством обработки содержащихся в запросе данных для изготовления вслепую денежной подписи соответствующим сумме кредитования денежным секретным ключом и доставляет их отправителю денежного запроса, который осуществляет проверку правильности доставленных ему данных для демаскировки посредством их обработки денежным открытым ключом, соответствующим использованному оператором денежному секретному ключу, и принимает их в качестве данных для получения подписи платежного сертификата, в платежные данные дополнительно включают платежное поручение плательщика и подпись для этого платежного поручения, которую предварительно получают на выходе подписывающего устройства после введения в него платежного поручения и секретного ключа подписи используемого платежного сертификата, причем в платежное поручение включают сведения о получателе платежа, условия платежа и идентификатор используемого платежного сертификата, при проведении по меньшей мере одной операции открытия у оператора платежной системы счета получателя платежа дополнительно получатель платежа выбирает посредством датчика случайных чисел секретный ключ подписи счета и соответствующий открытый ключ подписи счета, причем открытый ключ подписи счета доставляют посредством коммуникационных сетей в платежный сервер оператора платежной системы, который связывает его с открываемым счетом, при формировании платежного поручения получателя платежа в него включают условия платежа, изготавливают подпись платежного поручения получателя платежа посредством обработки его

секретным ключом подписи счета получателя платежа, а изготовленную подпись доставляют посредством коммуникационных сетей в платежный сервер оператора платежной системы, при проведении платежной операции оператор платежной системы дополнительно включает в свой ответ на платежное поручение получателя платежа квитанцию получателя платежа, предварительно подписанную посредством введения ее и одного из секретных ключей подписи оператора платежной системы в подписывающее устройство, до кредитования получателя платежа дополнительно проверяют правильность подписи для платежного поручения плательщика посредством устройства для проверки подписи, в которое предварительно вводят платежное поручение и открытый ключ подписи используемого платежного сертификата, проверяют правильность подписи для платежного поручения получателя платежа посредством устройства для проверки подписи, в которое предварительно вводят платежное поручение получателя платежа и открытый ключ подписи счета получателя платежа, контролируют соответствие условий платежа, содержащихся в платежных поручениях, при кредитовании счета получателя платежа дополнительно осуществляют дебетование платежного счета, связанного с используемым при платеже платежным сертификатом, получатель платежа по полученному ответу оператора платежной системы на свое платежное поручение осуществляет проверку правильности подписи для квитанции получателя платежа посредством введения ее и открытого ключа подписи, соответствующего использованному секретному ключу подписи оператора платежной системы в устройство для проверки подписи, по выходу которого судит о проведении платежа, и доставляет плательщику данные, по которым плательщик судит о проведении платежа.

Указанный выше технический результат в частных случаях конкретной реализации может достигаться, кроме того, тем, что при выборе при выборе основы платежного сертификата в нее включают дополнительный номер, а проверку действительности основы платежного сертификата при проверке правильности доставленной подписи платежного сертификата осуществляют по совпадению номера платежного сертификате и преобразованного посредством вычислителя наперед заданной односторонней функции дополнительного номера, причем выбор посредством датчика случайных чисел основы платежного сертификата, удовлетворяющей выбранному критерию действительности основ платежных сертификатов, осуществляют посредством выбора односторонней функции, выбором посредством датчика случайных чисел дополнительного номера, а номер получают посредством обработки выбранного дополнительного номера выбранной односторонней функцией.

Кроме того, при включении основу платежного сертификата идентификатора открытого ключа подписи платежного сертификата, в качестве этого идентификатора используют сам открытый ключ подписи платежного сертификата.

В частности, при включении в основу платежного сертификата идентификатор открытого ключа подписи платежного сертификата включают в основу в качестве дополнительного номера.

Помимо этого, перед включением в платежные данные платежного поручение плательщика осуществляют его шифрование одним из открытых ключей для шифрования оператора платежной системы, а оператор платежной системы производит дешифрование полученного от получателя платежа платежного поручения плательщика секретным ключом оператора платежной системы, соответствующим использованному плательщиком открытому ключу для шифрования.

Более того, оператор платежной системы осуществляет шифрование своего ответа на платежное поручение получателя платежа.

Кроме этого, в условия платежа, содержащиеся в платежном поручении плательщика, включают данные обязательства получателя платежа перед плательщиком.

Более того, при подготовке плательщиком платежных данных производят обработку данных обязательства получателя платежа перед плательщиком наперед заданной маскирующей функцией, а данные, полученные при этой обработке, включают в подготавливаемое платежное поручение плательщика, получатель платежа производит обработку данных обязательства получателя платежа перед плательщиком наперед заданной маскирующей функцией, а данные, полученные при этой обработке, включают в платежное поручение получателя платежа.

В частности, наперед заданную маскирующую функцию выбирают произвольно из множества односторонних функций.

Помимо этого, получатель платежа подписывает данные обязательства получателя платежа перед плательщиком одним из своих секретных ключей для подписи, получатель платежа до платежной операции проверяет подпись получателя для данных обязательства получателя платежа перед плательщиком.

Кроме того, при проведении по меньшей мере одной операции пополнения платежного устройства в качестве источника кредитования используют счет плательщика, который предварительно кредитуют при по меньшей мере одной платежной операции.

Помимо этого, при проведении по меньшей мере одной операции пополнения платежного устройства в качестве источника кредитования используют банковскую карточку.

Более того, при открытии платежного счета, связанного с авторизуемым платежном сертификатом, производят его предварительное дебетование.

В частности, при операции пополнения платежного сертификата формирование денежного запроса производят в соответствии с единой для всех денежных запросов структурой.

Помимо этого, подпись авторизуемого платежного сертификата изготавливают посредством понижения уровня имеющейся у плательщика подписи платежного сертификата.

В частности, при проведении платежной операции в качестве плательщика выступает получатель платежа.

Более того, оператор платежной системы может иметь по меньшей мере два платежных сервера .

Сущность способа проведения платежей по седьмому варианту состоит в том же, что и по третьему варианту, за исключением того, что плательщику получает подпись платежного сертификата посредством промежуточного плательщика, который производит платеж со своего счета на платежный сертификат плательщика. При этом промежуточный плательщик применяет дополнительную маскировку и, соответственно демаскировку проходящих через него данных для денежной подписи.

Единая совокупность признаков седьмого варианта заявленного способа, перечисленных выше, связана причинно-следственной связью с ранее изложенным техническим результатом изобретения, заключающемся в том, что при проведении платежей по открытым телекоммуникационным сетям денежные интересы каждого участника защищены от злоупотреблений всех других участников, причем плательщики и получатели платежей имеют возможность защиты своей приватности. Помимо этого доступны платежи в диапазоне от микроплатежей до платежей бизнес-уровня, время проведения платежа зависит только от быстроты действия сетевых соединений, но не от суммы платежа, число клиентов, которые могут быть обслужены оператором платежной системы, растет пропорционально его

ресурсам.

Указанный выше технический результат при осуществлении способа проведения платежей по седьмому варианту достигается, в частности, тем, что плательщик защищен от нечестного оператора платежной системы тем, что последний обязан отчитываться о проведенных им расходах по платежному сертификату подписанным платежным поручением плательщика, приватность плательщика защищена процедурой изготовления подписи платежного сертификата вслепую, а приватность получателя платежа может быть защищена тем, что при открытии счета получатель платежа не обязан сообщать никаких сведений, позволяющих определить его личность. Диапазон платежей и независимость времени проведения платежей обеспечены независимость суммы платежа от номинальных стоимостей, соответствующих денежным ключам. Рост числа клиентов пропорционально ресурсам оператора платежной системы обеспечен тем, что с помощью одного платежного сертификата можно проводить большое число платежей, а число используемых платежных сертификатов может быть ограничено стоимостью операции открытия платежного счета и операции изготовления вслепую денежной подписи.

Ниже заявитель приводит пример конкретной реализации способа проведения платежей по седьмому варианту.

Пример 14

В этом примере используются обозначения и соглашения, принятые в примере 10. Банк, плательщик и продавец действуют также как и в примере 10, за исключением того, что плательщик при пополнении своего платежного устройства доставляет замаскированные как и в примере 4 данные X' промежуточному плательщику, который производит их дополнительную маскировку и, соответственно, демаскировку полученных от банка данных для демаскировки точно так, как плательщик производит маскировку и демаскировку в примере 4.

В качестве других частных случаев способа по седьмому варианту заявитель отмечает возможность реализации в виде многих иных комбинаций зависимых пунктов 94-109, а также возможность шифрования, дешифрования и перекодировки данных при их передаче по коммуникационным сетям, которые не меняют сущности заявленного изобретения.

Кроме того, оператор платежной системы при авторизации платежного сертификата может проверять подпись платежного сертификата как открытыми так и секретными денежными ключами. Помимо этого, при ошибках работы коммуникационных сетей при проведении вовлеченных в проведение платежа операций, такие операции могут быть повторены до их успешного завершения без ущерба для вовлеченных сторон.

Предложенные варианты заявленного способа проведения платежей реализуются заявленным устройством.

Устройство для проведения платежей, содержащее платежное устройство, приемное устройство и платежный сервер, соединенные посредством телекоммуникационных сетей, причем платежное устройство содержит блоки маскировки и демаскировки, платежный сервер содержит блок хранения счетов и блок обработки денежного запроса с блоком денежной подписи, причем выход блока маскировки соединен со входом данных подписи блока денежной подписи, выход которого соединен с входом данных демаскировки блока демаскировки, платежное устройство содержит блок формирования денежного запроса, блок обработки ответа на денежный запрос, генератор ключей, блок проверки денежной подписи, вычислитель односторонней функции, отличается тем, что платежный сервер

дополнительно содержит генератор денежных ключей, выход которого соединен со входом записи блока хранения ключей, блок хранения платежных счетов, блок обработки запросов об открытии счета, блок обработки запроса на кредитование платежного счета, блок проведения платежа, платежное устройство дополнительно содержит генератор основы платежного сертификата, блок формирования запросов об открытии счета, блок обработки ответов на запрос об открытии счета, блок формирования запроса на кредитование платежного счета, блок формирования платежных данных, приемное устройство дополнительно содержит блок формирования запросов об открытии счета, блок обработки ответов на запрос об открытии счета, блок формирования платежного поручения получателя, блок обработки ответа на платежное поручение получателя, причем генератор основы платежного сертификата платежного устройства соединен с блоком хранения платежного сертификата и содержит генератор ключей, выход открытого ключа которого соединен со входом вычислителя односторонней функции и со входом установки открытого ключа блока хранения платежного сертификата, а выход секретного ключа которого соединен со входом установки секретного ключа блока хранения платежного сертификата, выход вычислителя односторонней функции соединен со входом установки подписи блока хранения платежного сертификата, генератор основы платежного сертификата содержит схему установки нуля, соединенную со входом установки уровня блока хранения платежного сертификата, блок формирования запросов об открытии счета платежного устройства подсоединен к блоку обработки запросов об открытии счета платежного сервера, который соединен с блоком обработки ответов на запрос об открытии счета платежного устройства, причем блок формирования запросов об открытии счета содержит генератор ключей, выход открытого ключа которого соединен со входом блока обработки запросов об открытии счета и со входом открытого ключа блока обработки ответов на запрос об открытии счета, а выход секретного ключа которого соединен со входом секретного ключа блока обработки ответов на запрос об открытии счета, выход блока обработки запросов об открытии счета соединен с входом создания записи блока хранения счетов и с блоком подписи, выход которого соединен со входом блока обработки ответов на запрос об открытии счета, выход параметров счета которого соединен со входом установки параметров счета блока хранения счета, а выход секретного ключа которого соединен со входом установки секретного ключа блока хранения счета, причем блок обработки ответов на запрос об открытии счета содержит блок проверки подписи, вход подписи которого соединен с выходом блока подписи, а выход которого соединен со входом загрузки блока хранения счета, выход блока формирования денежного запроса платежного устройства подсоединен ко входу блока обработки денежного запроса платежного сервера, выход которого соединен со входом блока обработки ответов на денежный запрос платежного устройства, причем блок формирования денежного запроса содержит блок маскировки и блок подписи, соединен с блоком хранения платежного сертификата и блоком хранения счета, выход блока маскировки подсоединен ко входу конкантенатора, к другому входу которого подсоединен выход идентификатора счета блока хранения счета, а выход конкантенатора соединен со входом данных блока подписи, ко входу секретного ключа которого подсоединен выход секретного ключа блока хранения счета, а выход блока подписи соединен со входом блока обработки денежного запроса, который содержит блок проверки подписи, блок денежной подписи и соединен с блоком хранения счетов, причем выход блока проверки подписи соединен со входом загрузки блока денежной подписи и входом загрузки блока дебетования счета, блок обработки ответа на денежный запрос содержит блок проверки денежной подписи и блок демаскировки, причем выход проверки блока

денежной подписи соединен со входом загрузки подписи блока хранения платежного сертификата, выход блока демаскировки соединен со входом установки подписи блока хранения платежного сертификата, выход блока формирования запроса на кредитование платежного счета платежного устройства соединен со входом блока обработки запроса на кредитование платежного счета платежного сервера, причем блок формирования запроса на кредитование платежного счета соединен с блоком хранения платежного сертификата и содержит блок понижения уровня платежного сертификата, вход подписи которого соединен с выходом подписи блока хранения платежного сертификата, а выход которого соединен со входом блока обработки запроса на кредитование платежного счета, который соединен с блоком хранения платежных счетов и содержит блок проверки денежной подписи, причем выход блока проверки денежной подписи соединен со входом загрузки входа кредитования блока хранения платежных счетов, блок формирования запросов об открытии счета приемного устройства подсоединен к блоку обработки запросов об открытии счета платежного сервера, который соединен с блоком обработки ответов на запрос об открытии счета приемного устройства, причем блок формирования запросов об открытии счета содержит генератор ключей, выход открытого ключа которого соединен со входом блока обработки запросов об открытии счета и со входом открытого ключа блока обработки ответов на запрос об открытии счета, а выход секретного ключа которого соединен со входом секретного ключа блока обработки ответов на запрос об открытии счета, выход блока обработки запросов об открытии счета соединен с входом создания записи блока хранения счетов и с блоком подписи, выход которого соединен со входом блока обработки ответов на запрос об открытии счета, выход параметров счета которого соединен со входом установки параметров счета блока хранения счета, а выход секретного ключа которого соединен со входом установки секретного ключа блока хранения счета, причем блок обработки ответов на запрос об открытии счета содержит блок проверки подписи, вход подписи которого соединен с выходом блока подписи, а выход которого соединен со входом загрузки блока хранения счета, блок формирования платежных данных платежного устройства содержит блок формирования платежного поручения плательщика и соединен со входом блока формирования платежного поручения получателя приемного устройства, который соединен с блоком проведения платежа платежного сервера, выход которого соединен с блоком обработки ответа на платежное поручение получателя приемного устройства, причем блок формирования платежного поручения плательщика содержит блок подписи, вход секретного ключа которого соединен с выходом секретного ключа блока хранения платежного сертификата, а выход которого соединен со входом подсоединенного к выходу блока формирования платежных данных конкантенатора, блок формирования платежного поручения получателя содержит блок подписи, вход секретного ключа которого соединен с выходом секретного ключа блока хранения счета, выход блока подписи соединен со входом подсоединенного к выходу блока формирования платежного поручения получателя конкантенатора, к другому входу которого подсоединен выход блока формирования платежного поручения плательщика, выход конкантенатора соединен со входом блока проведения платежа, который содержит блок проверки подписей плательщика и получателя, блок подписи квитанции получателя и соединен с блоком хранения платежных счетов и блоком хранения счетов, причем выход блока проверки подписи плательщика и получателя соединен со входами загрузки блока дебетования платежного счета, блока кредитования счета и блока подписи квитанции получателя, выход которого соединен со входом блока обработки ответа на платежное поручение получателя, который содержит блок проверки подписи.

Указанный выше технический результат в частных случаях конкретной реализации заявленного устройства может достигаться, кроме того, тем, что выход блока формирования запроса на кредитование платежного счета соединен со входом конкантенатора блока формирования платежных данных, к другому входу которого подсоединен выход блока формирования платежного поручения.

Более того, платежное устройство может дополнительно содержать шифрующее устройство, ко входу которого подсоединен выход блока формирования запроса на кредитование платежного счета, причем выход шифрующего устройства соединен со входом конкантенатора блока формирования платежных данных.

Кроме этого, платежное устройство, приемное устройство и платежный сервер могут быть дополнительно снабжены шифрующими и дешифрующими устройствами, через которые проходят соединения платежного устройства и приемного устройства, платежного устройства и платежного сервера, приемного устройства и платежного сервера.

Сущность устройства для проведения платежей состоит в том, что с его помощью плательщик может создавать основы платежных сертификатов, пополнять свое платежное устройство, осуществлять платежи, получатель платежа может открывать счета и принимать платежи, а оператор платежной системы обслуживать проведение платежей.

Единая совокупность признаков заявленного устройства, перечисленных выше, связана причинно-следственной связью с ранее изложенным техническим результатом изобретения, заключающемся в том, что при проведении платежей по открытым телекоммуникационным сетям денежные интересы каждого участника защищены от злоупотреблений всех других участников, причем плательщики и получатели платежей имеют возможность защиты своей приватности, доступны платежи в диапазоне от микроплатежей до платежей бизнес-уровня, время проведения платежа зависит только от быстроты действия сетевых соединений, но не от суммы платежа, число клиентов, которые могут быть обслужены оператором платежной системы, растет пропорционально его ресурсам.

Ниже заявитель приводит пример конкретной реализации заявленного устройства для проведения платежей.

Пример 15

Пример проиллюстрирован Фиг.1-8. На Фиг.1 изображено устройство для проведения платежей, содержащее платежный сервер 1, платежное устройство 2 приемное устройство 3 и коммуникационные связи между ними.

На Фиг.2 изображены блоки, вовлеченные в операцию открытия счета, а именно блок формирования запроса об открытии счета 4, блок обработки запросов об открытии счета 5 и блок обработки ответов на запрос об открытии счета 6 . При этом выход 7 блока формирования запроса об открытии счета 4 соединен со входом 8 блока обработки запросов об открытии счета 5, выход 9 которого соединен со входом 10 блока обработки ответов на запрос об открытии счета 6. Блок формирования запроса об открытии счета содержит генератор ключей 11, выход открытого ключа 12 которого, соединен с выходом блока формирования запроса об открытии счета 7 и, тем самым, со входом 8 блока обработки запросов об открытии счета 5. При этом выход открытого ключа 12 блока формирования запроса об открытии счета 4 также соединен со входом открытого ключа 13 блока обработки ответов на запрос об открытии счета 6, а выход секретного ключа 14 соединен со входом секретного ключа 15. Выход 16 блока обработки запросов об открытии счета соединен с входом создания записи 17 блока хранения счетов 18 и с блоком подписи 19, посредством подсоединения выхода 9 ко входу данных 20. Выход подписи 21 блока подписи 19 соединен со входом 10 блока

обработки ответов на запрос об открытии счета 6. На Фиг.2 изображен также блок хранения счета 22, причем выход секретного ключа 23 блока обработки ответов на запрос об открытии счета 6 соединен со входом установки секретного ключа 24 блока хранения счета 22,а выход параметров счета 25 соединен со входом установки параметров счета 26. Блок обработки ответов на запрос об открытии счета 6 содержит блок проверки подписи 27 выход которого 28 соединен со входом загрузки 29 блока хранения счета 22.

На Фиг. 3 изображен содержащийся в платежном устройстве 2 генератор основы платежного сертификата 30, соединенный с блоком хранения платежного сертификата 31, содержащий генератор ключей 32 и вычислитель односторонней функции 33. При этом выход открытого ключа 34 генератора ключей 32 соединен со входом 35 вычислителя односторонней функции 33 и со входом установки открытого ключа 36 блока хранения платежного сертификата 31, а выход секретного ключа 37 генератора ключей 32 соединен со входом установки секретного ключа 38 блока хранения платежного сертификата 31. Выход 39 вычислителя односторонней функции 33 соединен со входом установки подписи 40 блока хранения платежного сертификата 31. Кроме того, изображен вход установки уровня 41 блока хранения платежного сертификата 31, а схема установки нуля не показана.

На Фиг. 4 изображены блоки, вовлеченные в операцию пополнения платежного устройства, а именно блок формирования денежного запроса 42, блок обработки денежного запроса 43 и блок обработки ответа на денежный запрос 44. При этом выход 45 блока формирования денежного запроса 42 соединен со входом 46 блока обработки денежного запроса 43, выход которого 47 соединен со входом 48 блока обработки ответа на денежный запрос 44. Блок формирования денежного запроса 42 содержит блок маскировки 49 и блок подписи 50, выход блока маскировки подсоединен ко входу конкантенатора 51, к другому входу которого подсоединен выход блока хранения счета 22, а выход которого соединен со входом данных блока подписи 50, причем ко входу секретного ключа блока подписи 50 подсоединен выход секретного ключа блока хранения счета 22. Блок обработки денежного запроса 43 содержит блок проверки подписи 52, блок денежной подписи 53 и блок дебетования счета 54. Блок обработки ответа на денежный запрос 44 содержит блок демаскировки 55 и блок проверки денежной подписи 56, соединенные с блоком хранения платежного сертификата 31. Блоки маскировки и демаскировки могут быть изготовлены как в [6].

На Фиг. 5 изображены блоки, вовлеченные в операцию кредитования платежного счета, а именно блок формирования запроса на кредитование платежного счета 57, блок обработки запроса на кредитование платежного счета 58, причем соединение между этими блоками показано пунктиром, так как оно может быть выполнено не напрямую, а через соединения обоих блоков с приемным устройством 3. Блок формирования запроса на кредитование платежного счета 57 соединен с блоком хранения платежного сертификата 31 и содержит блок понижения уровня платежного сертификата 59. Такой блок понижения уровня может быть реализован модулярным экспоненциатором. Блок обработки запроса на кредитование платежного счета 58 содержит блок проверки денежной подписи 61, причем выход блока проверки денежной подписи соединен со входом загрузки входа кредитования блока хранения платежных счетов 60.

На Фиг. 6 изображена схема осуществления платежной операции, причем соединения, используемые в ходе этой операции обозначены как 62, 63, 64, 65 в порядке их использования при этой операции.

На Фиг. 7 изображены блоки, вовлеченные во взаимодействие между платежным устройством 2 и приемным устройством 3 при выполнении платежной операции. Платежное устройство 2 содержит блок формирования платежных данных 66 и блок

формирования платежного поручения плательщика 67. Приемное устройство 3 содержит блок формирования платежного поручения получателя 68, блок обработки ответа на платежное поручение получателя 69, блок хранения счета 70. Блок формирования платежного поручения плательщика 67 содержит блок подписи 71, вход секретного ключа которого соединен с выходом секретного ключа блока хранения платежного сертификата 31, а выход которого соединен со входом подсоединенного к выходу блока формирования платежных данных 66 конкантенатора 72. Блок формирования платежного поручения получателя 68 содержит блок подписи 73, вход секретного ключа которого соединен с выходом секретного ключа блока хранения счета 70, выход блока подписи 73 соединен со входом подсоединенного к выходу блока формирования платежного поручения получателя конкантенатора 74, к другому входу 75 которого подсоединен выход блока формирования платежного поручения плательщика 67.

На Фиг. 8 изображены блоки, вовлеченные во взаимодействие между приемным устройством 3 и платежным сервером 1 при выполнении платежной операции. Выход конкантенатора 74 соединен со входом блока проведения платежа 76, который содержит блок проверки подписей плательщика и получателя 77, блок подписи квитанции получателя 78 и соединен с блоком хранения платежных счетов 60 и блоком хранения счетов 18, причем выход блока проверки подписи плательщика и получателя 77 соединен со входами загрузки блока дебетования платежного счета, блока кредитования счета и блока подписи квитанции получателя, выход которого соединен со входом блока обработки ответа на платежное поручение получателя 69, который содержит блок проверки подписи 79.

Конкретный пример работы вышеописанного устройства для проведения платежей должен быть ясен из данного описания и примеров реализации способа проведения платежей. При этом плательщик пользуется платежным устройством, получатель платежа приемным устройством, а оператор платежной системы платежным сервером.

В качестве других частных случаев заявленного устройства заявитель отмечает возможность его реализации в виде многих иных разбиений содержащихся в нем вспомогательных устройств на блоки, которые не меняют сущности заявленного изобретения. Также возможно выполнять соединения между блоками путем пропускания этих соединений через дополнительные устройства. Среди таких дополнительных устройств могут быть, в частности, шифровальные и дешифровальные устройства, а также кодирующие и декодирующие устройства. Кроме того, заявленное устройство может быть дополнено другими известными устройствами, в частности, устройствами для перевода неизвестного банку остатка платежного сертификата на другой платежный сертификат, устройствами, обеспечивающими межбанковские коммуникации при проведении платежей между клиентами разных банков, устройствами для обслуживания счетов, в том числе для зачисления поступивших извне денег на счет и для вывода денег со счета, перевода денег с банковских карточек, другими устройствами для изготовления вслепую денежной подписи, в частности неожидаемой подписи, устройствами задержки времени и анонимизации сетевых адресов

Проведенный заявителем анализ уровня техники установил, что аналоги, характеризующиеся совокупностями признаков, тождественными всем признакам заявленного изобретения по каждому варианту, отсутствуют, что свидетельствует о соответствии заявленного изобретения, представленного в семи вариантах способа и одном варианте устройства для проведения платежей, условию «новизны».

Результаты поиска известных технических решений в данной и смежных областях техники с целью выявления признаков, совпадающих с отличительными от прототипа

признаками заявленного изобретения, показали, что они не следуют явным образом из известного уровня техники.

На основе анализа известного уровня техники заявителем не выявлена известность влияния существенных признаков каждого из вариантов заявленного изобретения на достижение указанного выше технического результата, что свидетельствует о соответствии каждого из вариантов заявленного изобретения условию «изобретательский уровень».

В описании и формуле заявленного изобретения соблюдено требование единства изобретения, поскольку каждый из вариантов заявленного изобретения предназначен для получения одного и того же указанного выше технического результата.

СПИСОК ЛИТЕРАТУРЫ

[1] T. Okamoto, K. Ohta, Method and apparatus for implementing electronic cash, U.S. Patent 4,977,595, 11 Dec 1990.

[2] T. Okamoto, K. Ohta, Electronic cash system, U.S. Patent 5,224,162, 8 Jun 1992.

[3] D. N. Simon, Untraceble electronic cash, U.S. Patent 5,768,385, 16 Jun 1998.

[4] D. Chaum, Security Without Identification: Transaction Systems to Make Big Brother Obsolete, Communications of the ACM, vol. 28 no. 10, October 1985 pp. 1030-1044; D. Chaum, Security without Identification: Card Computers to make Big Brother Obsolete, Copyright 1987 by David Chaum, http://www.digicash.com/digicash/personnel/people/david.htm (прототип);

[5] D. Chaum, Online Cash Checks, Advances in Cryptology EUROCRYPT '89, J.J. Quisquater & J. Vandewalle (Eds.), Springer-Verlag, pp. 288-293..

[6] D. Chaum, Blind Signature Systems, U.S. Patent 4,759,063, 19 Jul 1988.

[7] D. Chaum, Blind Unanticipated Signature Systems, U.S. Patent 4,759,064, 19 Jul 1988.

[8] D. Chaum, Returned Value Blind Signature Systems, U.S. Patent 4,949,380, 14 Aug 1990.

[9] S. S. Rosen, Electronic-monetary system, U.S. Patent 5,453,601, 26 Sep 1991.

[10] S. S. Rosen, Electronic-monetary system, U.S. Patent 5,455,407, 3 Oct 1995.

[11] A. C. Payne, L. C. Stewart, D. J. Mackie, Network Sales System, U.S. Patent 5,715,314, 3 Feb, 1998.

[12] B. Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, John Wiley&Sons, New York, 2nd edition, 1996.

[13] A. J. Menezes, P. C. Van Oorshot, S. A. Vanstone, Handbook of Applied Cryptography, CRC Press, 1997.

Генеральный директор
ЗАО «Алкорсофт» Волков С.В.

Закрытое акционерное общество "Алкорсофт" Санкт-Петербург

Авторы:
Золотарев О. А.
Кузнецов И. В.
Мошонкин А. Г.
Смирнов А. Л.
Хамитов И. М.

Пояснительные материалы
к тексту описания заявки
на изобретение:

«СПОСОБ ПРОВЕДЕНИЯ ПЛАТЕЖЕЙ И УСТРОЙСТВО ДЛЯ ЕГО РЕАЛИЗАЦИИ (варианты)»

С целью упрощения текста данной заявки заявитель приводит в пояснительных материалах сведения об используемой в тексте терминологии, известной из опубликованных источников и связанной с криптографическими понятиями, такими как цифровые подписи, изготовление цифровой подписи вслепую, открытые и секретные ключи, RSA-подписи, односторонние функции.

1. Цифровая подпись широко используются на практике и играет роль, аналогичную роли обычной рукописной подписи. Однако, цифровая подпись имеет преимущества перед рукописной подписью состоящие в том, что, во-первых, достоверность цифровой подписи легко проверяема, а ее подделка весьма затруднительна, а, во-вторых, в том, что цифровая подпись легко может быть передана по телекоммуникационным каналам.

Цифровая подпись для некоторых исходных данных представляет из себя другие цифровые данные, удовлетворяющие заранее оговоренному свойству цифровой подписи. Под цифровыми данными (или просто данными) понимается произвольная информация, представленная в цифровой форме. Данные могут быть представлены (закодированы) в различных формах и могут быть перекодированы из одной формы в другую. Многочисленные конкретные способы кодировки и декодировки известны специалистам и не важны для существа дела.

Термин «подписывающая сторона» указывает субъекта, контролирующего изготовление цифровой подписи, а термин «податель» указывает субъекта, желающего получить цифровую подпись. Для изготовления цифровой подписи подписывающая сторона выбирает секретную функцию и соответствующую ей проверяющую функцию. Для изготовления цифровой подписи на исходных данных податель передает их подписывающей стороне, которая изготавливает цифровую подпись с помощью обработки исходных данных секретной функцией и передает изготовленную подпись подателю. Как податель, так и любая иная сторона, с помощью общеизвестной проверяющей функции, может проверить, удовлетворяют ли полученная от подписывающей стороны цифровая подпись свойству подписи для исходных данных.

Под секретным ключом подписи понимаются данные, которые позволяют изготавливать цифровую подпись, а под соответствующим секретному ключу открытым ключом понимаются данные, которые позволяют проверять правильность цифровой подписи. Под генератором ключей понимается устройство, позволяющее создавать секретные и соответствующие им открытые ключи. Известны многочисленные примеры таких генераторов. Более подробно о цифровых подписях можно узнать в [1], [2].

2. В некоторых приложениях для подателя желательно, чтобы цифровая подпись изготавливалась вслепую. Это название происходит от того, что подписывающая сторона в ходе изготовления цифровой подписи не получает информации об исходных данных и, тем самым, не видит то, что она подписывает. Фактически под изготовления вслепую цифровой подписи понимается такой изготовление подписи, при котором обеспечивается непрослеживаемость. Таким образом, сказать, что способ изготовления подписи обеспечивает непрослеживаемость, то же самое, что и назвать такой способ способом изготовления подписи вслепую.

Общий метод изготовления вслепую цифровой подписи для некоторых исходных данных состоит в том, что податель создает на основе исходных данных и случайного

маскировочного ключа замаскированные данные, которые предоставляет подписывающей стороне. Подписывающая сторона возвращает подателю результат обработки замаскированных данных, а податель завершает изготовление вслепую цифровой подписи для исходных данных, производя демаскировку результата обработки замаскированных данных.

Непрослеживаемость означает, что для подписывающей стороны, которая получит впоследствии подписи многих исходных данных, будут равновероятны все возможные соответствия между этими подписями и обработанными замаскированными данными. Непрослеживаемость обеспечивается тем, что множество всех замаскированных данных, созданных на основе одних выбранных исходных данных совпадает с аналогичным множеством для других случайно выбранных исходных данных. Разумеется, что на практике достаточно обеспечить достаточно малую вероятность несовпадения вышеуказанных множеств.

Первые известные способы изготовления цифровой подписи вслепую связаны именно с RSA-подписью и описаны [1], [2]. Кроме того, известны способы изготовления вслепую цифровой подписи обладающие дополнительными свойствами, например, неожидаемостью. Данное свойство означает, что подписывающая сторона сама выбирает секретный ключ, используемый при изготовлении подписи, и, тем самым, при маскировке данных для подписи получатель подписи не может использовать предварительное знание открытого ключа, соответствующего использованному при изготовлении подписи секретному ключу. Другие известные способы изготовления цифровой подписи вслепую описаны [3].

3. Под RSA-ключом понимаются данные, которые позволяют производить RSA-шифрование. Обычно RSA-ключ состоит из RSA-модуля N и RSA-экспоненты E. При этом результатом RSA-шифрования некоторых данных M, представленных целым числом в диапазоне от 0 до N-1, являются другие данные C, связанные с данными M соотношением $C \equiv M^E \bmod N$. Под открытым RSA-ключом понимается общедоступный RSA-ключ. Экспоненту открытого RSA-ключа называют открытой RSA-экспонентой. Секретный RSA-ключ, соответствующий открытому RSA-ключу (N, E), предназначен, в частности, для изготовления RSA-подписи, которая может быть проверена открытым RSA-ключом. Секретный RSA-ключ обычно представляет из себя пару (N, D), где D называется секретной RSA-экспонентой. Открытый RSA-ключ (N, E) соответствует секретному RSA-ключу (N, D), если выполнено условие $E \times D \equiv 1 \bmod \varphi(N)$, где $\varphi(N)$ функция Эйлера. Разумеется, в частных случаях, секретные и открытые RSA-ключи могут быть заданы иным набором данных, обеспечивающим необходимую функциональность. Например, секретный ключ может быть представлен секретными множителями и открытой RSA-экспонентой, а открытая RSA-экспонента может быть представлена, например, набором ее множителей с некоторыми кратностями.

Данные S являются цифровой RSA-подписью для данных M, если $M \equiv S^E \bmod N$. Неподделываемость такой подписи без обладания секретными ключами обеспечивается вычислительной неразрешимостью некоторых теоретико-числовых задач, в частности, задачи факторизации больших натуральных чисел. Более подробно о цифровой RSA-подписи и RSA-шифровании можно узнать в [1], [2].

4. Под односторонней функцией понимается преобразование данных, которое в вычислительном смысле практически необратимо. Известны многочисленные примеры таких функций и устройств для их вычисления [1], [2]. Широкий класс односторонних функции представляют так называемые хэш-функции. При этом, в зависимости от цели использования, на односторонние функции накладывают дополнительные требования, такие, например, как практическая невозможность найти два значения, имеющих один и тот же образ при односторонней функции. Такие односторонние функции иногда на-

зывают односторонними функциями без столкновений.

Также к классу односторонних функций принадлежат "односторонние функции с лазейкой". При этом такие функции не удовлетворяют требованию односторонности для стороны, владеющей некоторым секретом ("лазейкой"), позволяющим, например, обращать одностороннюю функцию. Тем не менее, если защита безопасности стороны, опубликовавшей такую функцию, основана на предположении, что для сторон, не владеющих "лазейкой" опубликованная функция является односторонней, то такую функцию также следует рассматривать как одностороннюю.

Для некоторых схем подписи, в частности для RSA-подписи, легко получить подпись под некоторыми случайными данными без знания соответствующего секретного ключа. Для предотвращения такой возможности в некоторых схемах цифровой подписи подписывающая сторона объявляет подпись правильной только в том случае, если в подлежащие подписи данные встроен образ односторонней функции от некоторого известного получателю подписи значения. В этом случае односторонняя функция предназначена для защиты подписывающей стороны и может иметь "лазейку", являющуюся секретом подписывающей стороны.

Кроме того, односторонние функции могут использоваться для идентификации данных без их раскрытия. Например, если сторона, контролирующая идентичность некоторых данных X и Y владеет только их образами при односторонней функции, которая является односторонней функцией без столкновений, а сами данные X и Y не доступны для контролирующей стороны, то эта сторона может сделать вывод, что совпадают и сами данные X и Y.

СПИСОК ЛИТЕРАТУРЫ

[1] B. Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, John Wiley&Sons, New York, 2nd edition, 1996.

[2] A. J. Menezes, P. C. Van Oorshot, S. A. Vanstone, Handbook of Applied Cryptography, CRC Press, 1997.

[3] D. Pointcheval, J. Stern, Provably Secure Blind Signature, Lectures Notes in Computer Science, 1163, 1996, Springer, p. 252-265.

Генеральный директор
ЗАО «Алкорсофт» Волков С.В.

Закрытое акционерное общество "Алкорсофт" Санкт-Петербург

Авторы:
Золотарев О. А.
Кузнецов И. В.
Мошонкин А. Г.
Смирнов А. Л.
Хамитов И. М.

ФОРМУЛА ИЗОБРЕТЕНИЯ

1. Способ проведения платежей, заключающийся в выборе оператором платежной системы денежных секретных ключей и соответствующих денежных открытых ключей посредством генератора ключей, проведении по меньшей мере одной операции пополнения платежного устройства, при которой плательщик создает посредством датчика случайных чисел по меньшей мере одной основу платежного сертификата, которая включает его номер, и формирует денежный запрос, включающий замаскированный номер созданной основы платежного сертификата в качестве данных для изготовления вслепую денежной подписи, и доставляют его посредством коммуникационных сетей в платежный сервер оператора платежной системы, который по полученному денежному запросу определяет источник и сумму кредитования, создает при изготовлении вслепую денежной подписи данные для демаскировки посредством введения содержащихся в запросе данных для изготовления вслепую денежной подписи и соответствующего сумме кредитования денежного секретного ключа в подписывающее устройство и доставляет посредством коммуникационных сетей созданные данные для демаскировки в платежное устройство плательщика, после чего изготавливают подпись платежного сертификата введением доставленных данных для демаскировки в демаскирующее устройство и осуществляют проверку правильности изготовленной подписи платежного сертификата введением ее и денежного открытого ключа, соответствующего использованному оператором денежному секретному ключу, в устройство для проверки подписи, проведении по меньшей мере одной операции открытия у оператора платежной системы счета получателя платежа, проведении плательщиком по меньшей мере одной платежной операции, при которой подпись и основу используемого при платеже платежного сертификата включают в платежные данные, доставляемые получателю платежа, который формирует свое платежное поручение, включающее полученные от плательщика подпись и основу платежного сертификата, и доставляет его посредством коммуникационных сетей в платежный сервер оператора платежной системы, который по платежеспособности используемого при платеже платежного сертификата осуществляет кредитование счета получателя платежа на основе его платежного поручения, причем при проверке платежеспособности используемого при платеже платежного сертификата оператор платежной системы проводит операцию его авторизации, при которой по наличию информации об авторизуемом платежном сертификате в информационном хранилище отказывают в авторизации, а по ее отсутствию осуществляют проверку правильности доставленной подписи платежного сертификата введением ее в устройство для проверки подписи, и в случае правильности заносят информацию об авторизуемом платежном сертификате в информационное хранилище, после чего формируют ответ оператора платежной системы на платежное поручение получателя платежа и доставляют его посредством коммуникационных сетей получателю платежа, который по ответу оператора платежной системы судит о проведении платежа, *отличающийся тем, что* в основу платежного сертификата дополнительно включают идентификатор открытого ключа подписи платежного сертификата, предварительно изготовленного совместно с соответствующим ему секретным ключом подписи посредством генератора ключей, причем открытый ключ подписи платежного сертификата доставляют посредством коммуникационных сетей в платежный сервер оператора платежной системы, в платежные данные дополнительно включают платежное поручение плательщика с подписью, которую предварительно получают на выходе подписывающего устройства после введения в него платежного поручения

плательщика и секретного ключа подписи используемого платежного сертификата, причем в платежное поручение плательщика включают сведения о получателе платежа, условия платежа и идентификатор используемого платежного сертификата, при проведении по меньшей мере одной операции открытия у оператора платежной системы счета получателя платежа дополнительно получатель платежа посредством генератора ключей выбирает секретный ключ подписи счета и соответствующий открытый ключ подписи счета, причем открытый ключ подписи счета доставляют посредством коммуникационных сетей в платежный сервер оператора платежной системы, который связывает его с открываемым счетом, при формировании платежного поручения получателя платежа в него включают условия платежа, изготавливают подпись платежного поручения получателя платежа посредством введения его и секретного ключа подписи счета получателя платежа в подписывающее устройство, а изготовленную подпись доставляют посредством коммуникационных сетей в платежный сервер оператора платежной системы, при проведении платежной операции оператор платежной системы дополнительно включает в свой ответ на платежное поручение получателя платежа квитанцию получателя платежа, предварительно подписанную посредством введения ее и одного из секретных ключей подписи оператора платежной системы в подписывающее устройство, до кредитования получателя платежа дополнительно проверяют правильность подписи для платежного поручения плательщика посредством устройства для проверки подписи, в которое предварительно вводят платежное поручение плательщика и открытый ключ подписи используемого платежного сертификата, в информационное хранилище при авторизации платежного сертификата заносят подписанное платежное поручение плательщика, проверяют правильность подписи для платежного поручения получателя платежа посредством устройства для проверки подписи, в которое предварительно вводят платежное поручение получателя платежа и открытый ключ подписи счета получателя платежа, контролируют соответствие условий платежа, содержащихся в платежных поручениях плательщика и получателя платежа, получатель платежа по полученному ответу оператора платежной системы на свое платежное поручение осуществляет проверку правильности подписи для квитанции получателя платежа посредством введения ее и открытого ключа подписи, соответствующего использованному секретному ключу подписи оператора платежной системы в устройство для проверки подписи, по выходу которого судит о проведении платежа, и доставляет плательщику данные, по которым плательщик судит о проведении платежа.

2. Способ проведения платежей по п. 1, *отличающийся тем, что* при выборе основы платежного сертификата в нее включают дополнительный номер, а проверку действительности основы платежного сертификата при проверке правильности доставленной подписи платежного сертификата осуществляют по совпадению номера платежного сертификате и преобразованного посредством вычислителя наперед заданной односторонней функции дополнительного номера, причем выбор посредством датчика случайных чисел основы платежного сертификата, удовлетворяющей выбранному критерию действительности основ платежных сертификатов, осуществляют посредством выбора односторонней функции, выбором посредством датчика случайных чисел дополнительного номера, а номер получают посредством обработки выбранного дополнительного номера выбранной односторонней функцией.

3. Способ проведения платежей по п. 1, *отличающийся тем, что* при включении основу платежного сертификата идентификатора открытого ключа подписи платежного сертификата, в качестве этого идентификатора используют сам открытый ключ

подписи платежного сертификата.

4. Способ проведения платежей по п. 1-3, *отличающийся тем, что* при включении в основу платежного сертификата идентификатор открытого ключа подписи платежного сертификата включают в основу в качестве дополнительного номера.

5. Способ проведения платежей по п. 1, *отличающийся тем, что* перед включением в платежные данные платежного поручение плательщика осуществляют его шифрование одним из открытых ключей для шифрования оператора платежной системы, а оператор платежной системы производит дешифрование полученного от получателя платежа платежного поручения плательщика секретным ключом оператора платежной системы, соответствующим использованному плательщиком открытому ключу для шифрования.

6. Способ проведения платежей по п. 1, *отличающийся тем, что* оператор платежной системы осуществляет шифрование своего ответа на платежное поручение получателя платежа.

7. Способ проведения платежей по п. 1, *отличающийся тем, что* в условия платежа, содержащиеся в платежном поручении плательщика, включают данные обязательства получателя платежа перед плательщиком.

8. Способ проведения платежей по п.п. 1, 7 *отличающийся тем, что* при подготовке плательщиком платежных данных производят обработку данных обязательства получателя платежа перед плательщиком наперед заданной маскирующей функцией, а данные, полученные при этой обработке, включают в подготавливаемое платежное поручение плательщика, получатель платежа производит обработку данных обязательства получателя платежа перед плательщиком наперед заданной маскирующей функцией, а данные, полученные при этой обработке, включают в платежное поручение получателя платежа.

9. Способ проведения платежей по п.п. 1, 7 - 8, *отличающийся тем, что* наперед заданную маскирующую функцию выбирают произвольно из множества односторонних функций.

10. Способ проведения платежей по п. 1, *отличающийся тем, что* получатель платежа подписывает данные обязательства получателя платежа перед плательщиком одним из своих секретных ключей для подписи, получатель платежа до платежной операции проверяет подпись получателя для данных обязательства получателя платежа перед плательщиком.

11. Способ проведения платежей по п. 1, *отличающийся тем, что* при проведении по меньшей мере одной операции пополнения платежного устройства в качестве источника кредитования используют счет плательщика, который предварительно кредитуют при по меньшей мере одной платежной операции.

12. Способ проведения платежей по п. 1, *отличающийся тем, что* при проведении по меньшей мере одной операции пополнения платежного устройства в качестве источника кредитования используют банковскую карточку.

13. Способ проведения платежей по п.п. 1-12 *отличающийся тем, что* при проведении платежной операции в качестве плательщика выступает получатель платежа.

14. Способ проведения платежей по п. 1-13, *отличающийся тем, что* оператор платежной системы включает по меньшей мере два платежных сервера.

15. Способ проведения платежей, заключающийся в выборе оператором платежной системы денежных секретных ключей и соответствующих денежных открытых ключей посредством генератора ключей, выборе плательщиком посредством датчика

случайных чисел по меньшей мере одной основы платежного сертификата, которая содержит номер платежного сертификата, являющийся одновременно и подписью нулевого уровня платежного сертификата, проведении по меньшей мере одной операции пополнения платежного устройства, при которой плательщик создает посредством датчика случайных чисел по меньшей мере одной основу платежного сертификата, которая включает его номер, и формирует денежный запрос, включающий замаскированный номер созданной основы платежного сертификата в качестве данных для изготовления вслепую денежной подписи, и доставляют его посредством коммуникационных сетей в платежный сервер оператора платежной системы, который по полученному денежному запросу определяет источник и сумму кредитования, создает при изготовлении вслепую денежной подписи данные для демаскировки посредством введения содержащихся в запросе данных для изготовления вслепую денежной подписи и соответствующего сумме кредитования денежного секретного ключа в подписывающее устройство и доставляет посредством коммуникационных сетей созданные данные для демаскировки в платежное устройство плательщика, после чего изготавливают подпись платежного сертификата введением доставленных данных для демаскировки в демаскирующее устройство и осуществляют проверку правильности изготовленной подписи платежного сертификата введением ее и денежного открытого ключа, соответствующего использованному оператором денежному секретному ключу, в устройство для проверки подписи, проведении по меньшей мере одной операции авторизации оператором платежной системы платежного сертификата, подпись которого плательщик доставляет посредством коммуникационных сетей в платежный сервер оператора платежной системы, который осуществляет проверку правильности доставленной подписи платежного сертификата введением ее в устройство для проверки подписи, проведении по меньшей мере одной операции открытия у оператора платежной системы счета получателя платежа, проведении плательщиком по меньшей мере одной платежной операции, при которой подпись и основу используемого при платеже платежного сертификата включают в платежные данные, доставляемые получателю платежа, который формирует свое платежное поручение, включающее полученные от плательщика подпись и основу платежного сертификата, и доставляет его посредством коммуникационных сетей в платежный сервер оператора платежной системы, который по платежеспособности используемого при платеже платежного сертификата осуществляет кредитование счета получателя платежа на основе его платежного поручения, формирует свой ответ на платежное поручение получателя платежа и доставляет его получателю платежа, который по ответу оператора платежной системы судит о проведении платежа, *отличающийся тем, что* в основу платежного сертификата дополнительно включают идентификатор открытого ключа подписи платежного сертификата, предварительно изготовленного совместно с соответствующим ему секретным ключом подписи посредством генератора ключей, причем открытый ключ подписи платежного сертификата доставляют посредством коммуникационных сетей в платежный сервер оператора платежной системы, который при проведении операции авторизации дополнительно осуществляет поиск платежного счета, связанного с авторизуемым им платежном сертификатом, и в случае отсутствия такого счета, открывает его, а при наличии такого счета производит его кредитование на основе уровней авторизованных платежных сертификатов, связанных с данным счетом, доставляемую оператору платежной системы подпись авторизуемого им платежного сертификата плательщик изготавливает по соответствующим этому платежному сертификату данным для получения посредством демаскировки подписи платежного сертификата, причем уровень изготавливаемой подписи выбирают произвольно в пределах уровня секретного ключа, использованного для изготовления данных для получения

посредством демаскировки подписи платежного сертификата, в платежные данные дополнительно включают платежное поручение плательщика с подписью, которую предварительно получают на выходе подписывающего устройства после введения в него платежного поручения плательщика и секретного ключа подписи используемого платежного сертификата, причем в платежное поручение плательщика включают сведения о получателе платежа, условия платежа и идентификатор используемого платежного сертификата, при проведении по меньшей мере одной операции открытия у оператора платежной системы счета получателя платежа дополнительно получатель платежа выбирает посредством датчика случайных чисел секретный ключ подписи счета и соответствующий открытый ключ подписи счета, причем открытый ключ подписи счета доставляют посредством коммуникационных сетей в платежный сервер оператора платежной системы, который связывает его с открываемым счетом, при формировании платежного поручения получателя платежа в него включают условия платежа, изготавливают подпись платежного поручения получателя платежа посредством обработки его секретным ключом подписи счета получателя платежа, а изготовленную подпись доставляют посредством коммуникационных сетей в платежный сервер оператора платежной системы, при проведении платежной операции оператор платежной системы дополнительно включает в свой ответ на платежное поручение получателя платежа квитанцию получателя платежа, предварительно подписанную посредством введения ее и одного из секретных ключей подписи оператора платежной системы в подписывающее устройство, до кредитования получателя платежа дополнительно проверяют правильность подписи для платежного поручения плательщика посредством устройства для проверки подписи, в которое предварительно вводят платежное поручение плательщика и открытый ключ подписи используемого платежного сертификата, проверяют правильность подписи для платежного поручения получателя платежа посредством устройства для проверки подписи, в которое предварительно вводят платежное поручение получателя платежа и открытый ключ подписи счета получателя платежа, контролируют соответствие условий платежа, содержащихся в платежных поручениях плательщика и получателя платежа, при кредитовании счета получателя платежа дополнительно осуществляют дебетование платежного счета, связанного с используемым при платеже платежным сертификатом, получатель платежа по полученному ответу оператора платежной системы на свое платежное поручение осуществляет проверку правильности подписи для квитанции получателя платежа посредством введения ее и открытого ключа подписи, соответствующего использованному секретному ключу подписи оператора платежной системы в устройство для проверки подписи, по выходу которого судит о проведении платежа, и доставляет плательщику данные, по которым плательщик судит о проведении платежа.

16. Способ проведения платежей по п. 15, *отличающийся тем, что* при выборе основы платежного сертификата в нее включают дополнительный номер, а проверку действительности основы платежного сертификата при проверке правильности доставленной подписи платежного сертификата осуществляют по совпадению номера платежного сертификате и преобразованного посредством вычислителя наперед заданной односторонней функции дополнительного номера, причем выбор посредством датчика случайных чисел основы платежного сертификата, удовлетворяющей выбранному критерию действительности основ платежных сертификатов, осуществляют посредством выбора односторонней функции, выбором посредством датчика случайных чисел дополнительного номера, а номер получают посредством обработки выбранного дополнительного номера выбранной односторонней функцией.

17. Способ проведения платежей по п. 15, *отличающийся тем, что* при включении основу платежного сертификата идентификатора открытого ключа подписи платежного сертификата, в качестве этого идентификатора используют сам открытый ключ подписи платежного сертификата.

18. Способ проведения платежей по п. 15-17, *отличающийся тем, что* при включении в основу платежного сертификата идентификатор открытого ключа подписи платежного сертификата включают в основу в качестве дополнительного номера.

19. Способ проведения платежей по п. 15, *отличающийся тем, что* перед включением в платежные данные платежного поручение плательщика осуществляют его шифрование одним из открытых ключей для шифрования оператора платежной системы, а оператор платежной системы производит дешифрование полученного от получателя платежа платежного поручения плательщика секретным ключом оператора платежной системы, соответствующим использованному плательщиком открытому ключу для шифрования.

20. Способ проведения платежей по п. 15, *отличающийся тем, что* оператор платежной системы осуществляет шифрование своего ответа на платежное поручение получателя платежа.

21. Способ проведения платежей по п. 15, *отличающийся тем, что* в условия платежа, содержащиеся в платежном поручении плательщика, включают данные обязательства получателя платежа перед плательщиком.

22. Способ проведения платежей по п.п. 15, 21 *отличающийся тем, что* при подготовке плательщиком платежных данных производят обработку данных обязательства получателя платежа перед плательщиком наперед заданной маскирующей функцией, а данные, полученные при этой обработке, включают в подготавливаемое платежное поручение плательщика, получатель платежа производит обработку данных обязательства получателя платежа перед плательщиком наперед заданной маскирующей функцией, а данные, полученные при этой обработке, включают в платежное поручение получателя платежа.

23. Способ проведения платежей по п.п. 15, 21 - 22, *отличающийся тем, что* наперед заданную маскирующую функцию выбирают произвольно из множества односторонних функций.

24. Способ проведения платежей по п. 15, *отличающийся тем, что* получатель платежа подписывает данные обязательства получателя платежа перед плательщиком одним из своих секретных ключей для подписи, получатель платежа до платежной операции проверяет подпись получателя для данных обязательства получателя платежа перед плательщиком.

25. Способ проведения платежей по п. 15, *отличающийся тем, что* при проведении по меньшей мере одной операции пополнения платежного устройства в качестве источника кредитования используют счет плательщика, который предварительно кредитуют при по меньшей мере одной платежной операции.

26. Способ проведения платежей по п. 15, *отличающийся тем, что* при проведении по меньшей мере одной операции пополнения платежного устройства в качестве источника кредитования используют банковскую карточку.

27. Способ проведения платежей по п. 15, *отличающийся тем, что* при открытии платежного счета, связанного с авторизуемым платежном сертификатом, производят его предварительное дебетование.

28. Способ проведения платежей по п.п. 15-27, *отличающийся тем, что* при проведении платежной операции в качестве плательщика выступает получатель платежа.

29. Способ проведения платежей по п.п. 15-28, *отличающийся тем, что* имеется по меньшей мере два платежных сервера оператора платежной системы.

30. Способ проведения платежей, заключающийся в выборе оператором платежной системы денежных секретных ключей и соответствующих денежных открытых ключей посредством генератора ключей, выборе плательщиком посредством датчика случайных чисел по меньшей мере одной основы платежного сертификата, которая содержит номер платежного сертификата, являющийся одновременно и подписью нулевого уровня платежного сертификата, проведении по меньшей мере одной операции пополнения платежного устройства, при которой плательщик создает посредством датчика случайных чисел по меньшей мере одной основу платежного сертификата, которая включает его номер, и формирует денежный запрос, включающий замаскированный номер созданной основы платежного сертификата в качестве данных для изготовления вслепую денежной подписи, и доставляют его посредством коммуникационных сетей в платежный сервер оператора платежной системы, который по полученному денежному запросу определяет источник и сумму кредитования, создает при изготовлении вслепую денежной подписи данные для демаскировки посредством введения содержащихся в запросе данных для изготовления вслепую денежной подписи и соответствующего сумме кредитования денежного секретного ключа в подписывающее устройство и доставляет посредством коммуникационных сетей созданные данные для демаскировки в платежное устройство плательщика, после чего осуществляют проверку правильности доставленных данных для демаскировки посредством их обработки денежным открытым ключом, соответствующим использованному оператором денежному секретному ключу, и принимает их в качестве данных для получения подписи платежного сертификата, проведении по меньшей мере одной операции авторизации оператором платежной системы платежного сертификата, подпись которого доставляют посредством коммуникационных сетей в платежный сервер оператора платежной системы, который осуществляет проверку правильности доставленной подписи платежного сертификата введением ее в устройство для проверки подписи, проведении по меньшей мере одной операции открытия у оператора платежной системы счета получателя платежа, проведении плательщиком по меньшей мере одной платежной операции, при которой подпись и основу используемого при платеже платежного сертификата включают в платежные данные, доставляемые получателю платежа, который формирует свое платежное поручение, включающее полученные от плательщика подпись и основу платежного сертификата, и доставляет его посредством коммуникационных сетей в платежный сервер оператора платежной системы, который по платежеспособности используемого при платеже платежного сертификата осуществляет кредитование счета получателя платежа на основе его платежного поручения, формирует свой ответ на платежное поручение получателя платежа и доставляет его получателю платежа, который по ответу оператора платежной системы судит о проведении платежа, *отличающийся тем, что* в основу платежного сертификата дополнительно включают идентификатор открытого ключа подписи платежного сертификата, предварительно изготовленного совместно с соответствующим ему секретным ключом подписи посредством генератора ключей, причем открытый ключ подписи платежного сертификата доставляют посредством коммуникационных сетей в платежный сервер оператора платежной системы, который при проведении операции авторизации дополнительно осуществляет поиск

платежного счета, связанного с авторизуемым им платежном сертификатом, и в случае отсутствия такого счета, открывает его, а при наличии такого счета производит его кредитование на основе уровней авторизованных платежных сертификатов, связанных с данным счетом, доставляемую оператору платежной системы подпись авторизуемого им платежного сертификата плательщик изготавливает по соответствующим этому платежному сертификату данным для получения посредством демаскировки подписи платежного сертификата, причем уровень изготавливаемой подписи выбирают произвольно в пределах уровня секретного ключа, использованного для изготовления данных для получения посредством демаскировки подписи платежного сертификата, дополнительно по меньшей мере один из плательщиков проводит по меньшей мере одну операцию пополнения платежного устройства посредством операции пополнения платежного сертификата, при которой выбирают платежный сертификат и формируют денежный запрос, включающий данные для изготовления вслепую денежной подписи, в качестве которых берут замаскированную подпись платежного сертификата наибольшего уровня, предварительно изготовленную посредством демаскировки данных для получения подписи платежного сертификата, и доставляют его в платежный сервер оператора платежной системы, который по полученному денежному запросу определяет источник и сумму кредитования по денежному запросу, создает при изготовлении вслепую денежной подписи данные для демаскировки посредством обработки содержащихся в запросе данных для изготовления вслепую денежной подписи соответствующим сумме кредитования денежным секретным ключом и доставляет их отправителю денежного запроса, который осуществляет проверку правильности доставленных ему данных для демаскировки посредством их обработки денежным открытым ключом, соответствующим использованному оператором денежному секретному ключу, и принимает их в качестве данных для получения подписи платежного сертификата, в платежные данные дополнительно включают платежное поручение плательщика и подпись для этого платежного поручения, которую предварительно получают на выходе подписывающего устройства после введения в него платежного поручения и секретного ключа подписи используемого платежного сертификата, причем в платежное поручение включают сведения о получателе платежа, условия платежа и идентификатор используемого платежного сертификата, при проведении по меньшей мере одной операции открытия у оператора платежной системы счета получателя платежа дополнительно получатель платежа выбирает посредством датчика случайных чисел секретный ключ подписи счета и соответствующий открытый ключ подписи счета, причем открытый ключ подписи счета доставляют посредством коммуникационных сетей в платежный сервер оператора платежной системы, который связывает его с открываемым счетом, при формировании платежного поручения получателя платежа в него включают условия платежа, изготавливают подпись платежного поручения получателя платежа посредством обработки его секретным ключом подписи счета получателя платежа, а изготовленную подпись доставляют посредством коммуникационных сетей в платежный сервер оператора платежной системы, при проведении платежной операции оператор платежной системы дополнительно включает в свой ответ на платежное поручение получателя платежа квитанцию получателя платежа, предварительно подписанную посредством введения ее и одного из секретных ключей подписи оператора платежной системы в подписывающее устройство, до кредитования получателя платежа дополнительно проверяют правильность подписи для платежного поручения плательщика посредством устройства для проверки подписи, в которое предварительно вводят платежное поручение и открытый ключ подписи используемого платежного

сертификата, проверяют правильность подписи для платежного поручения получателя платежа посредством устройства для проверки подписи, в которое предварительно вводят платежное поручение получателя платежа и открытый ключ подписи счета получателя платежа, контролируют соответствие условий платежа, содержащихся в платежных поручениях, при кредитовании счета получателя платежа дополнительно осуществляют дебетование платежного счета, связанного с используемым при платеже платежным сертификатом, получатель платежа по полученному ответу оператора платежной системы на свое платежное поручение осуществляет проверку правильности подписи для квитанции получателя платежа посредством введения ее и открытого ключа подписи, соответствующего использованному секретному ключу подписи оператора платежной системы в устройство для проверки подписи, по выходу которого судит о проведении платежа, и доставляет плательщику данные, по которым плательщик судит о проведении платежа.

31. Способ проведения платежей по п. 30, *отличающийся тем, что* при выборе основы платежного сертификата в нее включают дополнительный номер, а проверку действительности основы платежного сертификата при проверке правильности доставленной подписи платежного сертификата осуществляют по совпадению номера платежного сертификате и преобразованного посредством вычислителя наперед заданной односторонней функции дополнительного номера, причем выбор посредством датчика случайных чисел основы платежного сертификата, удовлетворяющей выбранному критерию действительности основ платежных сертификатов, осуществляют посредством выбора односторонней функции, выбором посредством датчика случайных чисел дополнительного номера, а номер получают посредством обработки выбранного дополнительного номера выбранной односторонней функцией.

32. Способ проведения платежей по п. 30, *отличающийся тем, что* при включении основу платежного сертификата идентификатора открытого ключа подписи платежного сертификата, в качестве этого идентификатора используют сам открытый ключ подписи платежного сертификата.

33. Способ проведения платежей по п. 30-32, *отличающийся тем, что* при включении в основу платежного сертификата идентификатор открытого ключа подписи платежного сертификата включают в основу в качестве дополнительного номера.

34. Способ проведения платежей по п. 30, *отличающийся тем, что* перед включением в платежные данные платежного поручение плательщика осуществляют его шифрование одним из открытых ключей для шифрования оператора платежной системы, а оператор платежной системы производит дешифрование полученного от получателя платежа платежного поручения плательщика секретным ключом оператора платежной системы, соответствующим использованному плательщиком открытому ключу для шифрования.

35. Способ проведения платежей по п. 30, *отличающийся тем, что* оператор платежной системы осуществляет шифрование своего ответа на платежное поручение получателя платежа.

36. Способ проведения платежей по п. 30, *отличающийся тем, что* в условия платежа, содержащиеся в платежном поручении плательщика, включают данные обязательства получателя платежа перед плательщиком.

37. Способ проведения платежей по п.п. 30, 36 *отличающийся тем, что* при подготовке плательщиком платежных данных производят обработку данных

обязательства получателя платежа перед плательщиком наперед заданной маскирующей функцией, а данные, полученные при этой обработке, включают в подготавливаемое платежное поручение плательщика, получатель платежа производит обработку данных обязательства получателя платежа перед плательщиком наперед заданной маскирующей функцией, а данные, полученные при этой обработке, включают в платежное поручение получателя платежа.

38. Способ проведения платежей по п.п. 30, 36 - 37, *отличающийся тем, что* наперед заданную маскирующую функцию выбирают произвольно из множества односторонних функций.

39. Способ проведения платежей по п. 30, *отличающийся тем, что* получатель платежа подписывает данные обязательства получателя платежа перед плательщиком одним из своих секретных ключей для подписи, получатель платежа до платежной операции проверяет подпись получателя для данных обязательства получателя платежа перед плательщиком.

40. Способ проведения платежей по п. 30, *отличающийся тем, что* при проведении по меньшей мере одной операции пополнения платежного устройства в качестве источника кредитования используют счет плательщика, который предварительно кредитуют при по меньшей мере одной платежной операции.

41. Способ проведения платежей по п. 30, *отличающийся тем, что* при проведении по меньшей мере одной операции пополнения платежного устройства в качестве источника кредитования используют банковскую карточку.

42. Способ проведения платежей по п. 30, *отличающийся тем, что* при открытии платежного счета, связанного с авторизуемым платежном сертификатом, производят его предварительное дебетование.

43. Способ проведения платежей по п. 30, *отличающийся тем, что* при операции пополнения платежного сертификата формирование денежного запроса производят в соответствии с единой для всех денежных запросов структурой.

44. Способ проведения платежей по п. 30, *отличающийся тем, что* подпись авторизуемого платежного сертификата изготавливают посредством понижения уровня имеющейся у плательщика подписи платежного сертификата.

45. Способ проведения платежей по п.п. 30-44, *отличающийся тем, что* при проведении платежной операции в качестве плательщика выступает получатель платежа.

46. Способ проведения платежей по п.п. 30-45, *отличающийся тем, что* имеется по меньшей мере два платежных сервера оператора платежной системы.

47. Способ проведения платежей, заключающийся в выборе оператором платежной системы денежных секретных ключей и соответствующих денежных открытых ключей посредством генератора ключей, выборе плательщиком посредством датчика случайных чисел по меньшей мере одной основы платежного сертификата, которая содержит номер платежного сертификата, являющийся одновременно и подписью нулевого уровня платежного сертификата, проведении по меньшей мере одной операции пополнения платежного устройства, при которой плательщик создает посредством датчика случайных чисел по меньшей мере одной основу платежного сертификата, которая включает его номер, и формирует денежный запрос, включающий замаскированный номер созданной основы платежного сертификата в качестве данных для изготовления вслепую денежной подписи, и доставляют его посредством коммуникационных сетей в платежный сервер оператора платежной

системы, который по полученному денежному запросу определяет источник и сумму кредитования, создает при изготовлении вслепую денежной подписи данные для демаскировки посредством введения содержащихся в запросе данных для изготовления вслепую денежной подписи и соответствующего сумме кредитования денежного секретного ключа в подписывающее устройство и доставляет посредством коммуникационных сетей созданные данные для демаскировки в платежное устройство плательщика, после чего изготавливают подпись платежного сертификата введением доставленных данных для демаскировки в демаскирующее устройство и осуществляют проверку правильности изготовленной подписи платежного сертификата введением ее и денежного открытого ключа, соответствующего использованному оператором денежному секретному ключу, в устройство для проверки подписи, проведении по меньшей мере одной операции авторизации оператором платежной системы платежного сертификата, подпись которого плательщик доставляет посредством коммуникационных сетей в платежный сервер оператора платежной системы, который осуществляет проверку правильности доставленной подписи платежного сертификата введением ее в устройство для проверки подписи, проведении по меньшей мере одной операции открытия у оператора платежной системы счета получателя платежа, проведении плательщиком по меньшей мере одной платежной операции, при которой подпись и основу используемого при платеже платежного сертификата включают в платежные данные, доставляемые получателю платежа, который формирует свое платежное поручение, включающее полученные от плательщика подпись и основу платежного сертификата, и доставляет его посредством коммуникационных сетей в платежный сервер оператора платежной системы, который по платежеспособности используемого при платеже платежного сертификата осуществляет кредитование счета получателя платежа на основе его платежного поручения, формирует свой ответ на платежное поручение получателя платежа и доставляет его получателю платежа, который по ответу оператора платежной системы судит о проведении платежа, *отличающийся тем, что* в основу платежного сертификата дополнительно включают идентификатор открытого ключа подписи платежного сертификата, предварительно изготовленного совместно с соответствующим ему секретным ключом подписи посредством генератора ключей, причем открытый ключ подписи платежного сертификата доставляют посредством коммуникационных сетей в платежный сервер оператора платежной системы, который при проведении операции авторизации дополнительно осуществляет поиск платежного счета, связанного с авторизуемым им платежном сертификатом, и в случае отсутствия такого счета, открывает его, а при наличии такого счета производит его кредитование на основе уровней авторизованных платежных сертификатов, связанных с данным счетом, дополнительно по меньшей мере один из плательщиков проводит по меньшей мере одну операцию перевода с одного из платежных сертификатов на другой, один из которых выбирают в качестве исходного платежного сертификата, а другой в качестве целевого платежного сертификата, формируют денежный запрос, включающий данные для изготовления вслепую денежной подписи, в качестве которых берут предварительно изготовленную замаскированную подпись целевого платежного сертификата наибольшего уровня, и платежное поручение плательщика с подписью, которую предварительно получают на выходе подписывающего устройства после введения в него платежного поручения плательщика и секретного ключа подписи исходного платежного сертификата, причем в платежное поручение плательщика включают идентификатор исходного платежного сертификата и сумму перевода, денежный запрос доставляют посредством коммуникационных сетей в платежный сервер оператора платежной системы, который проверяет правильность подписи для платежного поручения плательщика посредством устройства для проверки подписи, в которое предварительно вводят платежное

поручение плательщика и открытый ключ подписи исходного платежного сертификата, осуществляют кредитование целевого платежного сертификата, при котором производят дебетование платежного счета, связанного с исходным платежным сертификатом, создают при изготовлении вслепую денежной подписи данные для демаскировки посредством обработки содержащихся в денежном запросе данных для изготовления вслепую денежной подписи денежным секретным ключом, соответствующим сумме кредитования целевого платежного сертификата, и доставляют их плательщику, который осуществляет проверку правильности доставленных ему данных для демаскировки посредством их обработки денежным открытым ключом, соответствующим использованному оператором платежной системы денежному секретному ключу, и принимает их в качестве данных для получения подписи целевого платежного сертификата, доставляемую оператору платежной системы подпись авторизуемого им платежного сертификата плательщик изготавливает по соответствующим этому платежному сертификату данным для получения посредством демаскировки подписи платежного сертификата, причем уровень изготавливаемой подписи выбирают произвольно в пределах уровня секретного ключа, использованного для изготовления данных для получения посредством демаскировки подписи платежного сертификата, в платежные данные дополнительно включают платежное поручение плательщика с подписью, которую предварительно получают на выходе подписывающего устройства после введения в него платежного поручения плательщика и секретного ключа подписи используемого платежного сертификата, причем в платежное поручение плательщика включают сведения о получателе платежа, условия платежа и идентификатор используемого платежного сертификата, при проведении по меньшей мере одной операции открытия у оператора платежной системы счета получателя платежа дополнительно получатель платежа выбирает посредством датчика случайных чисел секретный ключ подписи счета и соответствующий открытый ключ подписи счета, причем открытый ключ подписи счета доставляют посредством коммуникационных сетей в платежный сервер оператора платежной системы, который связывает его с открываемым счетом, при формировании платежного поручения получателя платежа в него включают условия платежа, изготавливают подпись платежного поручения получателя платежа посредством обработки его секретным ключом подписи счета получателя платежа, а изготовленную подпись доставляют посредством коммуникационных сетей в платежный сервер оператора платежной системы, при проведении платежной операции оператор платежной системы дополнительно включает в свой ответ на платежное поручение получателя платежа квитанцию получателя платежа, предварительно подписанную посредством введения ее и одного из секретных ключей подписи оператора платежной системы в подписывающее устройство, до кредитования получателя платежа дополнительно проверяют правильность подписи для платежного поручения плательщика посредством устройства для проверки подписи, в которое предварительно вводят платежное поручение плательщика и открытый ключ подписи используемого платежного сертификата, проверяют правильность подписи для платежного поручения получателя платежа посредством устройства для проверки подписи, в которое предварительно вводят платежное поручение получателя платежа и открытый ключ подписи счета получателя платежа, контролируют соответствие условий платежа, содержащихся в платежных поручениях плательщика и получателя платежа, при кредитовании счета получателя платежа дополнительно осуществляют дебетование платежного счета, связанного с используемым при платеже платежным сертификатом, получатель платежа по полученному ответу оператора платежной системы на свое платежное поручение осуществляет проверку правильности подписи для квитанции получателя платежа посредством введения ее и открытого ключа

подписи, соответствующего использованному секретному ключу подписи оператора платежной системы в устройство для проверки подписи, по выходу которого судит о проведении платежа, и доставляет плательщику данные, по которым плательщик судит о проведении платежа.

48. Способ проведения платежей по п. 47, *отличающийся тем, что* при выборе основы платежного сертификата в нее включают дополнительный номер, а проверку действительности основы платежного сертификата при проверке правильности доставленной подписи платежного сертификата осуществляют по совпадению номера платежного сертификате и преобразованного посредством вычислителя наперед заданной односторонней функции дополнительного номера, причем выбор посредством датчика случайных чисел основы платежного сертификата, удовлетворяющей выбранному критерию действительности основ платежных сертификатов, осуществляют посредством выбора односторонней функции, выбором посредством датчика случайных чисел дополнительного номера, а номер получают посредством обработки выбранного дополнительного номера выбранной односторонней функцией.

49. Способ проведения платежей по п. 47, *отличающийся тем, что* при включении основу платежного сертификата идентификатора открытого ключа подписи платежного сертификата, в качестве этого идентификатора используют сам открытый ключ подписи платежного сертификата.

50. Способ проведения платежей по п. 47-49, *отличающийся тем, что* при включении в основу платежного сертификата идентификатор открытого ключа подписи платежного сертификата включают в основу в качестве дополнительного номера.

51. Способ проведения платежей по п. 47, *отличающийся тем, что* перед включением в платежные данные платежного поручение плательщика осуществляют его шифрование одним из открытых ключей для шифрования оператора платежной системы, а оператор платежной системы производит дешифрование полученного от получателя платежа платежного поручения плательщика секретным ключом оператора платежной системы, соответствующим использованному плательщиком открытому ключу для шифрования.

52. Способ проведения платежей по п. 47, *отличающийся тем, что* оператор платежной системы осуществляет шифрование своего ответа на платежное поручение получателя платежа.

53. Способ проведения платежей по п. 47, *отличающийся тем, что* в условия платежа, содержащиеся в платежном поручении плательщика, включают данные обязательства получателя платежа перед плательщиком.

54. Способ проведения платежей по п.п. 47, 53 *отличающийся тем, что* при подготовке плательщиком платежных данных производят обработку данных обязательства получателя платежа перед плательщиком наперед заданной маскирующей функцией, а данные, полученные при этой обработке, включают в подготавливаемое платежное поручение плательщика, получатель платежа производит обработку данных обязательства получателя платежа перед плательщиком наперед заданной маскирующей функцией, а данные, полученные при этой обработке, включают в платежное поручение получателя платежа.

55. Способ проведения платежей по п.п. 47, 53 - 54, *отличающийся тем, что* наперед заданную маскирующую функцию выбирают произвольно из множества односторонних функций.

56. Способ проведения платежей по п. 47, *отличающийся тем, что* получатель платежа подписывает данные обязательства получателя платежа перед плательщиком одним из своих секретных ключей для подписи, получатель платежа до платежной операции проверяет подпись получателя для данных обязательства получателя платежа перед плательщиком.

57. Способ проведения платежей по п. 47, *отличающийся тем, что* при проведении по меньшей мере одной операции пополнения платежного устройства в качестве источника кредитования используют счет плательщика, который предварительно кредитуют при по меньшей мере одной платежной операции.

58. Способ проведения платежей по п. 47, *отличающийся тем, что* при проведении по меньшей мере одной операции пополнения платежного устройства в качестве источника кредитования используют банковскую карточку.

59. Способ проведения платежей по п. 47, *отличающийся тем, что* при открытии платежного счета, связанного с авторизуемым платежном сертификатом, производят его предварительное дебетование.

60. Способ проведения платежей по п. 47, *отличающийся тем, что* при операции пополнения платежного сертификата формирование денежного запроса производят в соответствии с единой для всех денежных запросов структурой.

61. Способ проведения платежей по п. 47, *отличающийся тем, что* подпись авторизуемого платежного сертификата изготавливают посредством понижения уровня имеющейся у плательщика подписи платежного сертификата.

62. Способ проведения платежей по п.п. 47-61, *отличающийся тем, что* при проведении платежной операции в качестве плательщика выступает получатель платежа.

63. Способ проведения платежей по п.п. 47- 62, *отличающийся тем, что* имеется по меньшей мере два платежных сервера оператора платежной системы.

64. Способ проведения платежей, заключающийся в выборе оператором платежной системы денежных секретных ключей и соответствующих денежных открытых ключей посредством генератора ключей, проведении по меньшей мере одной операции пополнения платежного устройства, при которой плательщик создает посредством датчика случайных чисел по меньшей мере одной основу платежного сертификата, которая включает его номер, и получает подпись платежного сертификата посредством изготовления вслепую денежной подписи оператором платежной системы, проведении плательщиком по меньшей мере одной платежной операции, при которой подпись и основу используемого при платеже платежного сертификата включают в платежные данные, доставляемые получателю платежа, который формирует свое платежное поручение, включающее полученные от плательщика подпись и основу платежного сертификата, и доставляет его посредством коммуникационных сетей в платежный сервер оператора платежной системы, который по платежеспособности используемого при платеже платежного сертификата осуществляет кредитование счета получателя платежа на основе его платежного поручения, причем при проверке платежеспособности используемого при платеже платежного сертификата оператор платежной системы проводит операцию его авторизации, при которой по наличию информации об авторизуемом платежном сертификате в информационном хранилище отказывают в авторизации, а по ее отсутствию осуществляют проверку правильности доставленной подписи платежного сертификата введением ее в устройство для проверки подписи, и в случае правильности заносят информацию об авторизуемом платежном сертификате в

информационное хранилище, после чего формируют ответ оператора платежной системы на платежное поручение получателя платежа и доставляют его получателю платежа, который по ответу оператора платежной системы судит о проведении платежа, *отличающийся тем, что* в основу платежного сертификата дополнительно включают идентификатор открытого ключа подписи платежного сертификата, предварительно изготовленного совместно с соответствующим ему секретным ключом подписи посредством генератора ключей, причем открытый ключ подписи платежного сертификата доставляют посредством коммуникационных сетей в платежный сервер оператора платежной системы, в платежные данные дополнительно включают платежное поручение плательщика с подписью, которую предварительно получают на выходе подписывающего устройства после введения в него платежного поручения плательщика и секретного ключа подписи используемого платежного сертификата, причем в платежное поручение плательщика включают сведения о получателе платежа, условия платежа и идентификатор используемого платежного сертификата, при проведении операции пополнения платежного устройства плательщик дополнительно формирует платежное требование, включающее замаскированную подпись выбранного платежного сертификата в качестве данных для изготовления вслепую денежной подписи, и подписанное одним из секретных ключей подписи плательщика, и доставляет его промежуточному плательщику, который проверяет подпись для платежного требования открытым ключом подписи плательщика, соответствующим использованному секретному ключу подписи плательщика, формирует и доставляет в платежный сервер оператора платежной системы денежный запрос, который включает дополнительно замаскированную промежуточным плательщиком полученную от плательщика замаскированную подпись выбранного платежного сертификата и идентификатор счета промежуточного плательщика, причем денежный запрос подписывают секретным ключом счета промежуточного плательщика, а оператор платежной системы проверяет подпись денежного запроса промежуточного плательщика открытым ключом счета, идентификатор которого содержится в денежном запросе, осуществляет дебетование этого счета, создает при изготовлении вслепую денежной подписи данные для демаскировки, которые доставляют промежуточному плательщику, который осуществляет проверку правильности доставленных ему данных для демаскировки посредством их обработки денежным открытым ключом, соответствующим использованному оператором платежной системы денежному секретному ключу, производит их демаскировку, результат которой доставляют плательщику, который изготавливает подпись платежного сертификата демаскировкой полученных от промежуточного плательщика данных для демаскировки, при проведении по меньшей мере одной операции открытия у оператора платежной системы счета получателя платежа дополнительно получатель платежа выбирает посредством датчика случайных чисел секретный ключ подписи счета и соответствующий открытый ключ подписи счета, причем открытый ключ подписи счета доставляют посредством коммуникационных сетей в платежный сервер оператора платежной системы, который связывает его с открываемым счетом, при формировании платежного поручения получателя платежа в него включают условия платежа, изготавливают подпись платежного поручения получателя платежа посредством обработки его секретным ключом подписи счета получателя платежа, а изготовленную подпись доставляют посредством коммуникационных сетей в платежный сервер оператора платежной системы, при проведении платежной операции оператор платежной системы дополнительно включает в свой ответ на платежное поручение получателя платежа квитанцию получателя платежа, предварительно подписанную посредством введения ее и одного из секретных ключей

подписи оператора платежной системы в подписывающее устройство, до кредитования получателя платежа дополнительно проверяют правильность подписи для платежного поручения плательщика посредством устройства для проверки подписи, в которое предварительно вводят платежное поручение плательщика и открытый ключ подписи используемого платежного сертификата, в информационное хранилище при авторизации платежного сертификата заносят подписанное платежное поручение плательщика, проверяют правильность подписи для платежного поручения получателя платежа посредством устройства для проверки подписи, в которое предварительно вводят платежное поручение получателя платежа и открытый ключ подписи счета получателя платежа, контролируют соответствие условий платежа, содержащихся в платежных поручениях плательщика и получателя платежа, получатель платежа по полученному ответу оператора платежной системы на свое платежное поручение осуществляет проверку правильности подписи для квитанции получателя платежа посредством введения ее и открытого ключа подписи, соответствующего использованному секретному ключу подписи оператора платежной системы в устройство для проверки подписи, по выходу которого судит о проведении платежа, и доставляет плательщику данные, по которым плательщик судит о проведении платежа.

65. Способ проведения платежей по п. 64, *отличающийся тем, что* при выборе основы платежного сертификата в нее включают дополнительный номер, а проверку действительности основы платежного сертификата при проверке правильности доставленной подписи платежного сертификата осуществляют по совпадению номера платежного сертификате и преобразованного посредством вычислителя наперед заданной односторонней функции дополнительного номера, причем выбор посредством датчика случайных чисел основы платежного сертификата, удовлетворяющей выбранному критерию действительности основ платежных сертификатов, осуществляют посредством выбора односторонней функции, выбором посредством датчика случайных чисел дополнительного номера, а номер получают посредством обработки выбранного дополнительного номера выбранной односторонней функцией.

66. Способ проведения платежей по п. 64, *отличающийся тем, что* при включении основу платежного сертификата идентификатора открытого ключа подписи платежного сертификата, в качестве этого идентификатора используют сам открытый ключ подписи платежного сертификата.

67. Способ проведения платежей по п. 64-66, *отличающийся тем, что* при включении в основу платежного сертификата идентификатор открытого ключа подписи платежного сертификата включают в основу в качестве дополнительного номера.

68. Способ проведения платежей по п. 64, *отличающийся тем, что* перед включением в платежные данные платежного поручение плательщика осуществляют его шифрование одним из открытых ключей для шифрования оператора платежной системы, а оператор платежной системы производит дешифрование полученного от получателя платежа платежного поручения плательщика секретным ключом оператора платежной системы, соответствующим использованному плательщиком открытому ключу для шифрования.

69. Способ проведения платежей по п. 64, *отличающийся тем, что* оператор платежной системы осуществляет шифрование своего ответа на платежное поручение получателя платежа.

70. Способ проведения платежей по п. 64, *отличающийся тем, что* в условия платежа, содержащиеся в платежном поручении плательщика, включают данные обязательства

получателя платежа перед плательщиком.

71. Способ проведения платежей по п.п. 64, 70 *отличающийся тем, что* при подготовке плательщиком платежных данных производят обработку данных обязательства получателя платежа перед плательщиком наперед заданной маскирующей функцией, а данные, полученные при этой обработке, включают в подготавливаемое платежное поручение плательщика, получатель платежа производит обработку данных обязательства получателя платежа перед плательщиком наперед заданной маскирующей функцией, а данные, полученные при этой обработке, включают в платежное поручение получателя платежа.

72. Способ проведения платежей по п.п. 64, 70 - 71, *отличающийся тем, что* наперед заданную маскирующую функцию выбирают произвольно из множества односторонних функций.

73. Способ проведения платежей по п. 64, *отличающийся тем, что* получатель платежа подписывает данные обязательства получателя платежа перед плательщиком одним из своих секретных ключей для подписи, получатель платежа до платежной операции проверяет подпись получателя для данных обязательства получателя платежа перед плательщиком.

74. Способ проведения платежей по п. 64, *отличающийся тем, что* при проведении по меньшей мере одной операции пополнения платежного устройства в качестве источника кредитования используют счет плательщика, который предварительно кредитуют при по меньшей мере одной платежной операции.

75. Способ проведения платежей по п. 64, *отличающийся тем, что* при проведении по меньшей мере одной операции пополнения платежного устройства в качестве источника кредитования используют банковскую карточку.

76. Способ проведения платежей по п.п. 64-75, *отличающийся тем, что* при проведении платежной операции в качестве плательщика выступает получатель платежа.

77. Способ проведения платежей по п.п. 64-76, *отличающийся тем, что* имеется по меньшей мере два платежных сервера оператора платежной системы.

78. Способ проведения платежей, заключающийся в выборе оператором платежной системы денежных секретных ключей и соответствующих денежных открытых ключей посредством генератора ключей, выборе плательщиком посредством датчика случайных чисел по меньшей мере одной основы платежного сертификата, которая содержит номер платежного сертификата, являющийся одновременно и подписью нулевого уровня платежного сертификата, проведении по меньшей мере одной операции пополнения платежного устройства, при которой плательщик получает подпись платежного сертификата посредством изготовления вслепую денежной подписи оператором платежной системы, проведении по меньшей мере одной операции авторизации оператором платежной системы платежного сертификата, подпись которого плательщик доставляет посредством коммуникационных сетей в платежный сервер оператора платежной системы, который осуществляет проверку правильности доставленной подписи платежного сертификата введением ее в устройство для проверки подписи, проведении по меньшей мере одной операции открытия у оператора платежной системы счета получателя платежа, проведении плательщиком по меньшей мере одной платежной операции, при которой подпись и основу используемого при платеже платежного сертификата включают в платежные данные, доставляемые получателю платежа, который формирует свое платежное поручение, включающее полученные от плательщика подпись и основу платежного

сертификата, и доставляет его посредством коммуникационных сетей в платежный сервер оператора платежной системы, который по платежеспособности используемого при платеже платежного сертификата осуществляет кредитование счета получателя платежа на основе его платежного поручения, формирует свой ответ на платежное поручение получателя платежа и доставляет его получателю платежа, который по ответу оператора платежной системы судит о проведении платежа, *отличающийся тем, что* в основу платежного сертификата дополнительно включают идентификатор открытого ключа подписи платежного сертификата, предварительно изготовленного совместно с соответствующим ему секретным ключом подписи посредством генератора ключей, причем открытый ключ подписи платежного сертификата доставляют посредством коммуникационных сетей в платежный сервер оператора платежной системы, который при проведении операции авторизации дополнительно осуществляет поиск платежного счета, связанного с авторизуемым им платежном сертификатом, и в случае отсутствия такого счета, открывает его, а при наличии такого счета производит его кредитование на основе уровней авторизованных платежных сертификатов, связанных с данным счетом, доставляемую оператору платежной системы подпись авторизуемого им платежного сертификата плательщик изготавливает по соответствующим этому платежному сертификату данным для получения посредством демаскировки подписи платежного сертификата, причем уровень изготавливаемой подписи выбирают произвольно в пределах уровня секретного ключа, использованного для изготовления данных для получения посредством демаскировки подписи платежного сертификата, дополнительно по меньшей мере один из плательщиков проводит по меньшей мере одну операцию пополнения платежного устройства посредством перевода со счета промежуточного плательщика, при которой плательщик дополнительно формирует платежное требование, включающее замаскированную подпись выбранного платежного сертификата в качестве данных для изготовления вслепую денежной подписи, и подписанное одним из секретных ключей подписи плательщика, и доставляет его промежуточному плательщику, который проверяет подпись для платежного требования открытым ключом подписи плательщика, соответствующим использованному плательщиком секретному ключу подписи, формирует и доставляет в платежный сервер оператора платежной системы денежный запрос, который включает дополнительно замаскированную промежуточным плательщиком полученную от плательщика замаскированную подпись выбранного платежного сертификата и идентификатор счета промежуточного плательщика, причем денежный запрос подписывают секретным ключом счета промежуточного плательщика, а оператор платежной системы проверяет подпись денежного запроса промежуточного плательщика открытым ключом счета, идентификатор которого содержится в денежном запросе, осуществляет дебетование этого счета, создает при изготовлении вслепую денежной подписи данные для демаскировки, которые доставляют промежуточному плательщику, который осуществляет проверку правильности доставленных ему данных для демаскировки посредством их обработки денежным открытым ключом, соответствующим использованному оператором денежному секретному ключу, производит их демаскировку, результат которой доставляют плательщику, который изготавливает подпись платежного сертификата демаскировкой полученных от промежуточного плательщика данных для демаскировки, в платежные данные дополнительно включают платежное поручение плательщика с подписью, которую предварительно получают на выходе подписывающего устройства после введения в него платежного поручения и секретного ключа подписи используемого платежного сертификата, причем в платежное поручение включают сведения о получателе платежа, условия платежа и идентификатор используемого платежного сертификата, при проведении по меньшей

мере одной операции открытия у оператора платежной системы счета получателя платежа дополнительно получатель платежа выбирает посредством датчика случайных чисел секретный ключ подписи счета и соответствующий открытый ключ подписи счета, причем открытый ключ подписи счета доставляют посредством коммуникационных сетей в платежный сервер оператора платежной системы, который связывает его с открываемым счетом, при формировании платежного поручения получателя платежа в него включают условия платежа, изготавливают подпись платежного поручения получателя платежа посредством обработки его секретным ключом подписи счета получателя платежа, а изготовленную подпись доставляют посредством коммуникационных сетей в платежный сервер оператора платежной системы, при проведении платежной операции оператор платежной системы дополнительно включает в свой ответ на платежное поручение получателя платежа квитанцию получателя платежа, предварительно подписанную посредством введения ее и одного из секретных ключей подписи оператора платежной системы в подписывающее устройство, до кредитования получателя платежа дополнительно проверяют правильность подписи для платежного поручения плательщика посредством устройства для проверки подписи, в которое предварительно вводят платежное поручение плательщика и открытый ключ подписи используемого платежного сертификата, проверяют правильность подписи для платежного поручения получателя платежа посредством устройства для проверки подписи, в которое предварительно вводят платежное поручение получателя платежа и открытый ключ подписи счета получателя платежа, контролируют соответствие условий платежа, содержащихся в платежных поручениях плательщика и получателя платежа, при кредитовании счета получателя платежа дополнительно осуществляют дебетование платежного счета, связанного с используемым при платеже платежным сертификатом, получатель платежа по полученному ответу оператора платежной системы на свое платежное поручение осуществляет проверку правильности подписи для квитанции получателя платежа посредством введения ее и открытого ключа подписи, соответствующего использованному секретному ключу подписи оператора платежной системы в устройство для проверки подписи, по выходу которого судит о проведении платежа, и доставляет плательщику данные, по которым плательщик судит о проведении платежа.

79. Способ проведения платежей по п. 78, *отличающийся тем, что* при выборе основы платежного сертификата в нее включают дополнительный номер, а проверку действительности основы платежного сертификата при проверке правильности доставленной подписи платежного сертификата осуществляют по совпадению номера платежного сертификате и преобразованного посредством вычислителя наперед заданной односторонней функции дополнительного номера, причем выбор посредством датчика случайных чисел основы платежного сертификата, удовлетворяющей выбранному критерию действительности основ платежных сертификатов, осуществляют посредством выбора односторонней функции, выбором посредством датчика случайных чисел дополнительного номера, а номер получают посредством обработки выбранного дополнительного номера выбранной односторонней функцией.

80. Способ проведения платежей по п. 78, *отличающийся тем, что* при включении основу платежного сертификата идентификатора открытого ключа подписи платежного сертификата, в качестве этого идентификатора используют сам открытый ключ подписи платежного сертификата.

81. Способ проведения платежей по п. 78-80, *отличающийся тем, что* при включении в основу платежного сертификата идентификатор открытого ключа подписи платежного сертификата включают в основу в качестве дополнительного номера.

82. Способ проведения платежей по п. 78, *отличающийся тем, что* перед включением в платежные данные платежного поручение плательщика осуществляют его шифрование одним из открытых ключей для шифрования оператора платежной системы, а оператор платежной системы производит дешифрование полученного от получателя платежа платежного поручения плательщика секретным ключом оператора платежной системы, соответствующим использованному плательщиком открытому ключу для шифрования.

83. Способ проведения платежей по п. 78, *отличающийся тем, что* оператор платежной системы осуществляет шифрование своего ответа на платежное поручение получателя платежа.

84. Способ проведения платежей по п. 78, *отличающийся тем, что* в условия платежа, содержащиеся в платежном поручении плательщика, включают данные обязательства получателя платежа перед плательщиком.

85. Способ проведения платежей по п.п. 78, 84 *отличающийся тем, что* при подготовке плательщиком платежных данных производят обработку данных обязательства получателя платежа перед плательщиком наперед заданной маскирующей функцией, а данные, полученные при этой обработке, включают в подготавливаемое платежное поручение плательщика, получатель платежа производит обработку данных обязательства получателя платежа перед плательщиком наперед заданной маскирующей функцией, а данные, полученные при этой обработке, включают в платежное поручение получателя платежа.

86. Способ проведения платежей по п.п. 78, 84 - 85, *отличающийся тем, что* наперед заданную маскирующую функцию выбирают произвольно из множества односторонних функций.

87. Способ проведения платежей по п. 78, *отличающийся тем, что* получатель платежа подписывает данные обязательства получателя платежа перед плательщиком одним из своих секретных ключей для подписи, получатель платежа до платежной операции проверяет подпись получателя для данных обязательства получателя платежа перед плательщиком.

88. Способ проведения платежей по п. 78, *отличающийся тем, что* при проведении по меньшей мере одной операции пополнения платежного устройства в качестве источника кредитования используют счет плательщика, который предварительно кредитуют при по меньшей мере одной платежной операции.

89. Способ проведения платежей по п. 78, *отличающийся тем, что* при проведении по меньшей мере одной операции пополнения платежного устройства в качестве источника кредитования используют банковскую карточку.

90. Способ проведения платежей по п. 78, *отличающийся тем, что* при открытии платежного счета, связанного с авторизуемым платежном сертификатом, производят его предварительное дебетование.

91. Способ проведения платежей по п.п. 78-90, *отличающийся тем, что* при проведении платежной операции в качестве плательщика выступает получатель платежа.

92. Способ проведения платежей по п.п. 78-91, *отличающийся тем, что* имеется по меньшей мере два платежных сервера оператора платежной системы.

93. Способ проведения платежей, заключающийся в выборе оператором платежной системы денежных секретных ключей и соответствующих денежных открытых ключей

посредством генератора ключей, выборе плательщиком посредством датчика случайных чисел по меньшей мере одной основы платежного сертификата, которая содержит номер платежного сертификата, являющийся одновременно и подписью нулевого уровня платежного сертификата, проведении по меньшей мере одной операции пополнения платежного устройства, при которой плательщик получает подпись платежного сертификата посредством изготовления вслепую денежной подписи оператором платежной системы, проведении по меньшей мере одной операции авторизации оператором платежной системы платежного сертификата, подпись которого плательщик доставляет посредством коммуникационных сетей в платежный сервер оператора платежной системы, который осуществляет проверку правильности доставленной подписи платежного сертификата введением ее в устройство для проверки подписи, проведении по меньшей мере одной операции открытия у оператора платежной системы счета получателя платежа, проведении плательщиком по меньшей мере одной платежной операции, при которой подпись и основу используемого при платеже платежного сертификата включают в платежные данные, доставляемые получателю платежа, который формирует свое платежное поручение, включающее полученные от плательщика подпись и основу платежного сертификата, и доставляет его посредством коммуникационных сетей в платежный сервер оператора платежной системы, который по платежеспособности используемого при платеже платежного сертификата осуществляет кредитование счета получателя платежа на основе его платежного поручения, формирует свой ответ на платежное поручение получателя платежа и доставляет его получателю платежа, который по ответу оператора платежной системы судит о проведении платежа, *отличающийся тем, что* в основу платежного сертификата дополнительно включают идентификатор открытого ключа подписи платежного сертификата, предварительно изготовленного совместно с соответствующим ему секретным ключом подписи посредством генератора ключей, причем открытый ключ подписи платежного сертификата доставляют посредством коммуникационных сетей в платежный сервер оператора платежной системы, который при проведении операции авторизации дополнительно осуществляет поиск платежного счета, связанного с авторизуемым им платежном сертификатом, и в случае отсутствия такого счета, открывает его, а при наличии такого счета производит его кредитование на основе уровней авторизованных платежных сертификатов, связанных с данным счетом, доставляемую оператору платежной системы подпись авторизуемого им платежного сертификата плательщик изготавливает по соответствующим этому платежному сертификату данным для получения посредством демаскировки подписи платежного сертификата, причем уровень изготавливаемой подписи выбирают произвольно в пределах уровня секретного ключа, использованного для изготовления данных для получения посредством демаскировки подписи платежного сертификата, дополнительно по меньшей мере один из плательщиков проводит по меньшей мере одну операцию пополнения платежного устройства посредством перевода со счета промежуточного плательщика, при которой плательщик дополнительно формирует платежное требование, включающее замаскированную подпись выбранного платежного сертификата в качестве данных для изготовления вслепую денежной подписи, и подписанное одним из секретных ключей подписи плательщика, и доставляет его промежуточному плательщику, который проверяет подпись для платежного требования открытым ключом подписи плательщика, соответствующим использованному плательщиком секретному ключу подписи, формирует и доставляет в платежный сервер оператора платежной системы денежный запрос, который включает дополнительно замаскированную промежуточным плательщиком полученную от плательщика замаскированную подпись выбранного платежного сертификата и идентификатор счета промежуточного плательщика, причем

денежный запрос подписывают секретным ключом счета промежуточного плательщика, а оператор платежной системы проверяет подпись денежного запроса промежуточного плательщика открытым ключом счета, идентификатор которого содержится в денежном запросе, осуществляет дебетование этого счета, создает при изготовлении вслепую денежной подписи данные для демаскировки, которые доставляют промежуточному плательщику, который осуществляет проверку правильности доставленных ему данных для демаскировки посредством их обработки денежным открытым ключом, соответствующим использованному оператором денежному секретному ключу, производит их демаскировку, результат которой доставляют плательщику, который изготавливает подпись платежного сертификата демаскировкой полученных от промежуточного плательщика данных для демаскировки, дополнительно по меньшей мере один из плательщиков проводит по меньшей мере одну операцию пополнения платежного устройства посредством операции пополнения платежного сертификата, при которой выбирают платежный сертификат и формируют денежный запрос, включающий данные для изготовления вслепую денежной подписи, в качестве которых берут замаскированную подпись платежного сертификата наибольшего уровня, предварительно изготовленную посредством демаскировки данных для получения подписи платежного сертификата, и доставляют его в платежный сервер оператора платежной системы, который по полученному денежному запросу определяет источник и сумму кредитования по денежному запросу, создает при изготовлении вслепую денежной подписи данные для демаскировки посредством обработки содержащихся в запросе данных для изготовления вслепую денежной подписи соответствующим сумме кредитования денежным секретным ключом и доставляет их отправителю денежного запроса, который осуществляет проверку правильности доставленных ему данных для демаскировки посредством их обработки денежным открытым ключом, соответствующим использованному оператором денежному секретному ключу, и принимает их в качестве данных для получения подписи платежного сертификата, в платежные данные дополнительно включают платежное поручение плательщика и подпись для этого платежного поручения, которую предварительно получают на выходе подписывающего устройства после введения в него платежного поручения и секретного ключа подписи используемого платежного сертификата, причем в платежное поручение включают сведения о получателе платежа, условия платежа и идентификатор используемого платежного сертификата, при проведении по меньшей мере одной операции открытия у оператора платежной системы счета получателя платежа дополнительно получатель платежа выбирает посредством датчика случайных чисел секретный ключ подписи счета и соответствующий открытый ключ подписи счета, причем открытый ключ подписи счета доставляют посредством коммуникационных сетей в платежный сервер оператора платежной системы, который связывает его с открываемым счетом, при формировании платежного поручения получателя платежа в него включают условия платежа, изготавливают подпись платежного поручения получателя платежа посредством обработки его секретным ключом подписи счета получателя платежа, а изготовленную подпись доставляют посредством коммуникационных сетей в платежный сервер оператора платежной системы, при проведении платежной операции оператор платежной системы дополнительно включает в свой ответ на платежное поручение получателя платежа квитанцию получателя платежа, предварительно подписанную посредством введения ее и одного из секретных ключей подписи оператора платежной системы в подписывающее устройство, до кредитования получателя платежа дополнительно проверяют правильность подписи для платежного поручения плательщика посредством устройства для проверки подписи, в которое предварительно вводят платежное

поручение и открытый ключ подписи используемого платежного сертификата, проверяют правильность подписи для платежного поручения получателя платежа посредством устройства для проверки подписи, в которое предварительно вводят платежное поручение получателя платежа и открытый ключ подписи счета получателя платежа, контролируют соответствие условий платежа, содержащихся в платежных поручениях, при кредитовании счета получателя платежа дополнительно осуществляют дебетование платежного счета, связанного с используемым при платеже платежным сертификатом, получатель платежа по полученному ответу оператора платежной системы на свое платежное поручение осуществляет проверку правильности подписи для квитанции получателя платежа посредством введения ее и открытого ключа подписи, соответствующего использованному секретному ключу подписи оператора платежной системы в устройство для проверки подписи, по выходу которого судит о проведении платежа, и доставляет плательщику данные, по которым плательщик судит о проведении платежа.

94. Способ проведения платежей по п. 93, *отличающийся тем, что* при выборе основы платежного сертификата в нее включают дополнительный номер, а проверку действительности основы платежного сертификата при проверке правильности доставленной подписи платежного сертификата осуществляют по совпадению номера платежного сертификате и преобразованного посредством вычислителя наперед заданной односторонней функции дополнительного номера, причем выбор посредством датчика случайных чисел основы платежного сертификата, удовлетворяющей выбранному критерию действительности основ платежных сертификатов, осуществляют посредством выбора односторонней функции, выбором посредством датчика случайных чисел дополнительного номера, а номер получают посредством обработки выбранного дополнительного номера выбранной односторонней функцией.

95. Способ проведения платежей по п. 93, *отличающийся тем, что* при включении основу платежного сертификата идентификатора открытого ключа подписи платежного сертификата, в качестве этого идентификатора используют сам открытый ключ подписи платежного сертификата.

96. Способ проведения платежей по п. 93-95, *отличающийся тем, что* при включении в основу платежного сертификата идентификатор открытого ключа подписи платежного сертификата включают в основу в качестве дополнительного номера.

97. Способ проведения платежей по п. 93, *отличающийся тем, что* перед включением в платежные данные платежного поручение плательщика осуществляют его шифрование одним из открытых ключей для шифрования оператора платежной системы, а оператор платежной системы производит дешифрование полученного от получателя платежа платежного поручения плательщика секретным ключом оператора платежной системы, соответствующим использованному плательщиком открытому ключу для шифрования.

98. Способ проведения платежей по п. 93, *отличающийся тем, что* оператор платежной системы осуществляет шифрование своего ответа на платежное поручение получателя платежа.

99. Способ проведения платежей по п. 93, *отличающийся тем, что* в условия платежа, содержащиеся в платежном поручении плательщика, включают данные обязательства получателя платежа перед плательщиком.

100. Способ проведения платежей по п.п. 93, 99 *отличающийся тем, что* при подготовке плательщиком платежных данных производят обработку данных

обязательства получателя платежа перед плательщиком наперед заданной маскирующей функцией, а данные, полученные при этой обработке, включают в подготавливаемое платежное поручение плательщика, получатель платежа производит обработку данных обязательства получателя платежа перед плательщиком наперед заданной маскирующей функцией, а данные, полученные при этой обработке, включают в платежное поручение получателя платежа.

101. Способ проведения платежей по п.п. 93, 99 - 100, *отличающийся тем, что* наперед заданную маскирующую функцию выбирают произвольно из множества односторонних функций.

102. Способ проведения платежей по п. 93, *отличающийся тем, что* получатель платежа подписывает данные обязательства получателя платежа перед плательщиком одним из своих секретных ключей для подписи, получатель платежа до платежной операции проверяет подпись получателя для данных обязательства получателя платежа перед плательщиком.

103. Способ проведения платежей по п. 93, *отличающийся тем, что* при проведении по меньшей мере одной операции пополнения платежного устройства в качестве источника кредитования используют счет плательщика, который предварительно кредитуют при по меньшей мере одной платежной операции.

104. Способ проведения платежей по п. 93, *отличающийся тем, что* при проведении по меньшей мере одной операции пополнения платежного устройства в качестве источника кредитования используют банковскую карточку.

105. Способ проведения платежей по п. 93, *отличающийся тем, что* при открытии платежного счета, связанного с авторизуемым платежном сертификатом, производят его предварительное дебетование.

106. Способ проведения платежей по п. 93, *отличающийся тем, что* при операции пополнения платежного сертификата формирование денежного запроса производят в соответствии с единой для всех денежных запросов структурой.

107. Способ проведения платежей по п. 93, *отличающийся тем, что* подпись авторизуемого платежного сертификата изготавливают посредством понижения уровня имеющейся у плательщика подписи платежного сертификата.

108. Способ проведения платежей по п.п. 93-107, *отличающийся тем, что* при проведении платежной операции в качестве плательщика выступает получатель платежа.

109. Способ проведения платежей по п.п. 93-108, *отличающийся тем, что* имеется по меньшей мере два платежных сервера оператора платежной системы.

110. Устройство для проведения платежей, содержащее платежное устройство, приемное устройство и платежный сервер, соединенные посредством телекоммуникационных сетей, причем платежное устройство содержит блоки маскировки и демаскировки, платежный сервер содержит блок хранения счетов и блок обработки денежного запроса с блоком денежной подписи, причем выход блока маскировки соединен со входом данных подписи блока денежной подписи, выход которого соединен с входом данных демаскировки блока демаскировки, платежное устройство содержит блок формирования денежного запроса, блок обработки ответа на денежный запрос, генератор ключей, блок проверки денежной подписи, вычислитель односторонней функции, *отличающееся тем, что* платежный сервер дополнительно содержит генератор денежных ключей, выход которого соединен со входом записи блока хранения ключей, блок хранения платежных

счетов, блок обработки запросов об открытии счета, блок обработки запроса на кредитование платежного счета, блок проведения платежа, платежное устройство дополнительно содержит генератор основы платежного сертификата, блок формирования запросов об открытии счета, блок обработки ответов на запрос об открытии счета, блок формирования запроса на кредитование платежного счета, блок формирования платежных данных, приемное устройство дополнительно содержит блок формирования запросов об открытии счета, блок обработки ответов на запрос об открытии счета, блок формирования платежного поручения получателя, блок обработки ответа на платежное поручение получателя, причем генератор основы платежного сертификата платежного устройства соединен с блоком хранения платежного сертификата и содержит генератор ключей, выход открытого ключа которого соединен со входом вычислителя односторонней функции и со входом установки открытого ключа блока хранения платежного сертификата, а выход секретного ключа которого соединен со входом установки секретного ключа блока хранения платежного сертификата, выход вычислителя односторонней функции соединен со входом установки подписи блока хранения платежного сертификата, генератор основы платежного сертификата содержит схему установки нуля, соединенную со входом установки уровня блока хранения платежного сертификата, блок формирования запросов об открытии счета платежного устройства подсоединен к блоку обработки запросов об открытии счета платежного сервера, который соединен с блоком обработки ответов на запрос об открытии счета платежного устройства, причем блок формирования запросов об открытии счета содержит генератор ключей, выход открытого ключа которого соединен со входом блока обработки запросов об открытии счета и со входом открытого ключа блока обработки ответов на запрос об открытии счета, а выход секретного ключа которого соединен со входом секретного ключа блока обработки ответов на запрос об открытии счета, выход блока обработки запросов об открытии счета соединен с входом создания записи блока хранения счетов и с блоком подписи, выход которого соединен со входом блока обработки ответов на запрос об открытии счета, выход параметров счета которого соединен со входом установки параметров счета блока хранения счета, а выход секретного ключа которого соединен со входом установки секретного ключа блока хранения счета, причем блок обработки ответов на запрос об открытии счета содержит блок проверки подписи, вход подписи которого соединен с выходом блока подписи, а выход которого соединен со входом загрузки блока хранения счета, выход блока формирования денежного запроса платежного устройства подсоединен ко входу блока обработки денежного запроса платежного сервера, выход которого соединен со входом блока обработки ответов на денежный запрос платежного устройства, причем блок формирования денежного запроса содержит блок маскировки и блок подписи, соединен с блоком хранения платежного сертификата и блоком хранения счета, выход блока маскировки подсоединен ко входу конкантенатора, к другому входу которого подсоединен выход идентификатора счета блока хранения счета, а выход конкантенатора соединен со входом данных блока подписи, ко входу секретного ключа которого подсоединен выход секретного ключа блока хранения счета, а выход блока подписи соединен со входом блока обработки денежного запроса, который содержит блок проверки подписи, блок денежной подписи и соединен с блоком хранения счетов, причем выход блока проверки подписи соединен со входом загрузки блока денежной подписи и входом загрузки блока дебетования счета, блок обработки ответа на денежный запрос содержит блок проверки денежной подписи и блок демаскировки, причем выход проверки блока денежной подписи соединен со входом загрузки подписи блока хранения платежного сертификата, выход блока демаскировки

соединен со входом установки подписи блока хранения платежного сертификата, выход блока формирования запроса на кредитование платежного счета платежного устройства соединен со входом блока обработки запроса на кредитование платежного счета платежного сервера, причем блок формирования запроса на кредитование платежного счета соединен с блоком хранения платежного сертификата и содержит блок понижения уровня платежного сертификата, вход подписи которого соединен с выходом подписи блока хранения платежного сертификата, а выход которого соединен со входом блока обработки запроса на кредитование платежного счета, который соединен с блоком хранения платежных счетов и содержит блок проверки денежной подписи, причем выход блока проверки денежной подписи соединен со входом загрузки входа кредитования блока хранения платежных счетов, блок формирования запросов об открытии счета приемного устройства подсоединен к блоку обработки запросов об открытии счета платежного сервера, который соединен с блоком обработки ответов на запрос об открытии счета приемного устройства, причем блок формирования запросов об открытии счета содержит генератор ключей, выход открытого ключа которого соединен со входом блока обработки запросов об открытии счета и со входом открытого ключа блока обработки ответов на запрос об открытии счета, а выход секретного ключа которого соединен со входом секретного ключа блока обработки ответов на запрос об открытии счета, выход блока обработки запросов об открытии счета соединен с входом создания записи блока хранения счетов и с блоком подписи, выход которого соединен со входом блока обработки ответов на запрос об открытии счета, выход параметров счета которого соединен со входом установки параметров счета блока хранения счета, а выход секретного ключа которого соединен со входом установки секретного ключа блока хранения счета, причем блок обработки ответов на запрос об открытии счета содержит блок проверки подписи, вход подписи которого соединен с выходом блока подписи, а выход которого соединен со входом загрузки блока хранения счета, блок формирования платежных данных платежного устройства содержит блок формирования платежного поручения плательщика и соединен со входом блока формирования платежного поручения получателя приемного устройства, который соединен с блоком проведения платежа платежного сервера, выход которого соединен с блоком обработки ответа на платежное поручение получателя приемного устройства, причем блок формирования платежного поручения плательщика содержит блок подписи, вход секретного ключа которого соединен с выходом секретного ключа блока хранения платежного сертификата, а выход которого соединен со входом подсоединенного к выходу блока формирования платежных данных конкантенатора, блок формирования платежного поручения получателя содержит блок подписи, вход секретного ключа которого соединен с выходом секретного ключа блока хранения счета, выход блока подписи соединен со входом подсоединенного к выходу блока формирования платежного поручения получателя конкантенатора, к другому входу которого подсоединен выход блока формирования платежного поручения плательщика, выход конкантенатора соединен со входом блока проведения платежа, который содержит блок проверки подписей плательщика и получателя, блок подписи квитанции получателя и соединен с блоком хранения платежных счетов и блоком хранения счетов, причем выход блока проверки подписи плательщика и получателя соединен со входами загрузки блока дебетования платежного счета, блока кредитования счета и блока подписи квитанции получателя, выход которого соединен со входом блока обработки ответа на платежное поручение получателя, который содержит блок проверки подписи.

111. Устройство для проведения платежей по п. 110, *отличающееся тем, что* выход

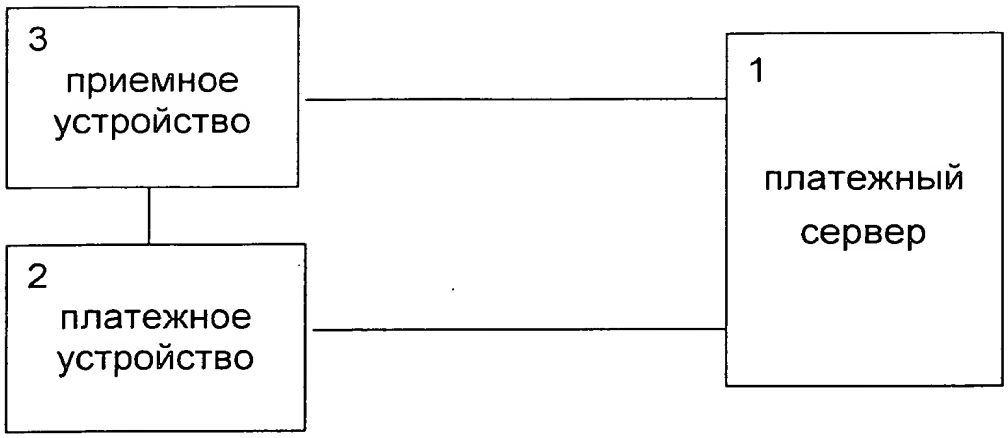
блока формирования запроса на кредитование платежного счета соединен со входом конкантенатора блока формирования платежных данных, к другому входу которого подсоединен выход блока формирования платежного поручения.

112. Устройство для проведения платежей по п. 111, *отличающееся тем, что* платежное устройство дополнительно содержит шифрующее устройство, ко входу которого подсоединен выход блока формирования запроса на кредитование платежного счета, причем выход шифрующего устройства соединен со входом конкантенатора блока формирования платежных данных.

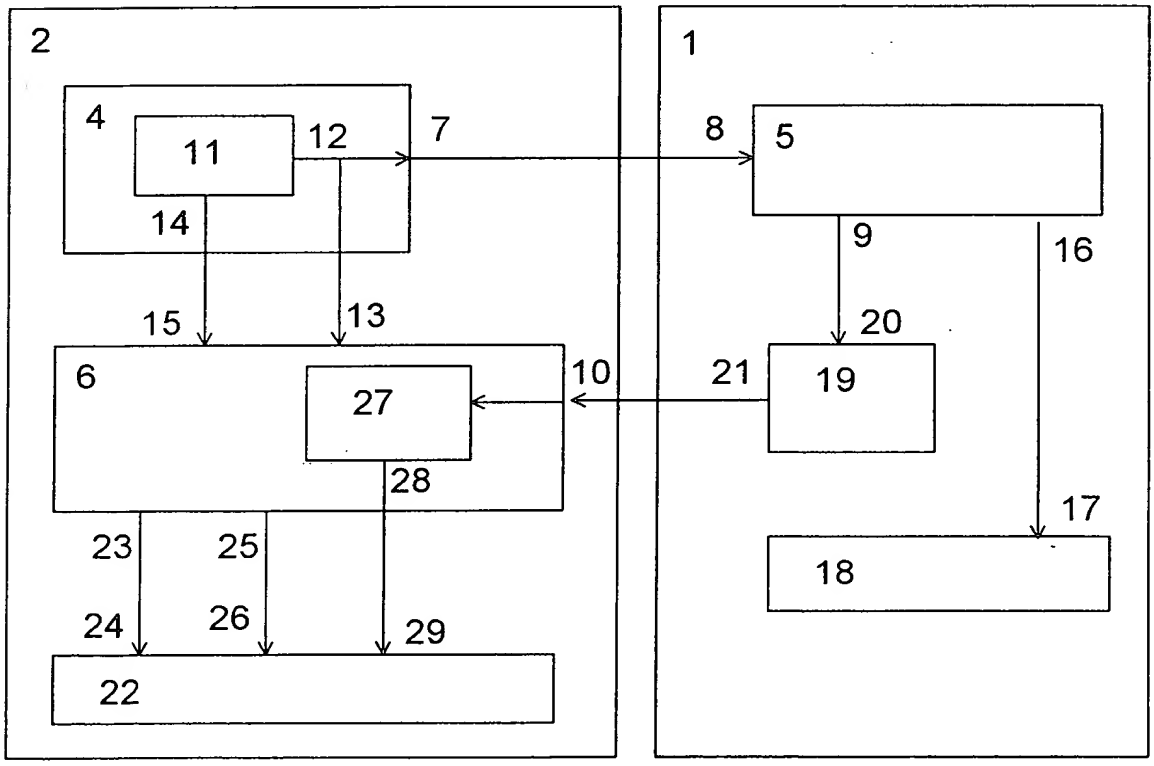
113. Устройство для проведения платежей по п. 110, *отличающееся тем, что* платежное устройство, приемное устройство и платежный сервер дополнительно снабжены шифрующими и дешифрующими устройствами, через которые проходят соединения платежного устройства и приемного устройства, платежного устройства и платежного сервера, приемного устройства и платежного сервера.

Генеральный директор
ЗАО «Алкорсофт» Волков С.В.

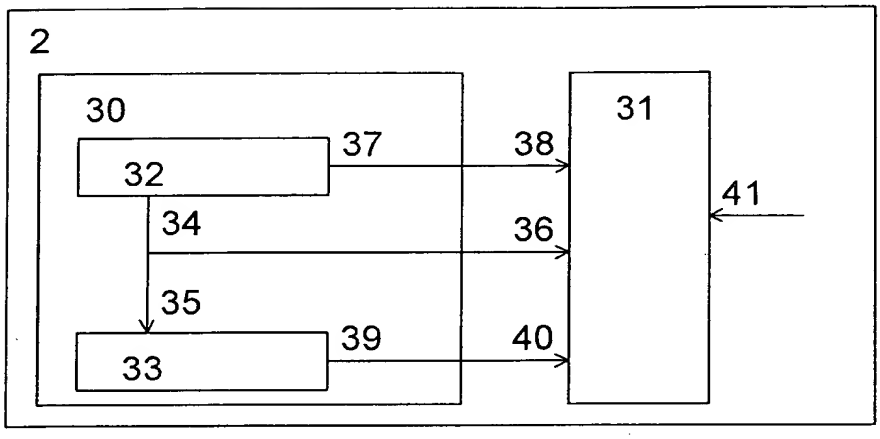
Авторы:
Золотарев О. А.
Кузнецов И. В.
Мошонкин А. Г.
Смирнов А. Л.
Хамитов И. М.


3
приемное
устройство
1
платежный
сервер
2
платежное
устройство

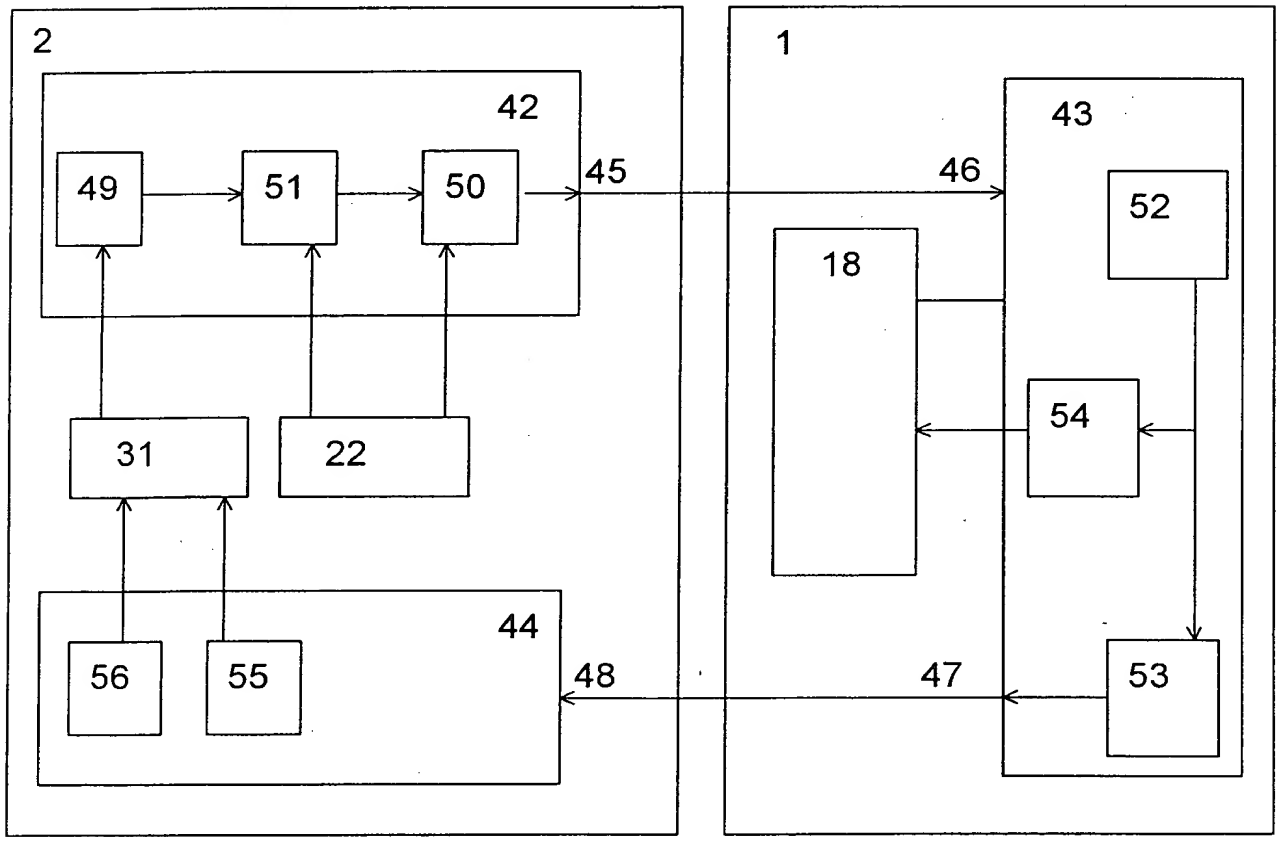
ФИГ. 1


2
1
4
11
12
7
8
5
14
9
16
15
13
20
6
27
10
21
19
28
17
23
25
18
24
26
29
22

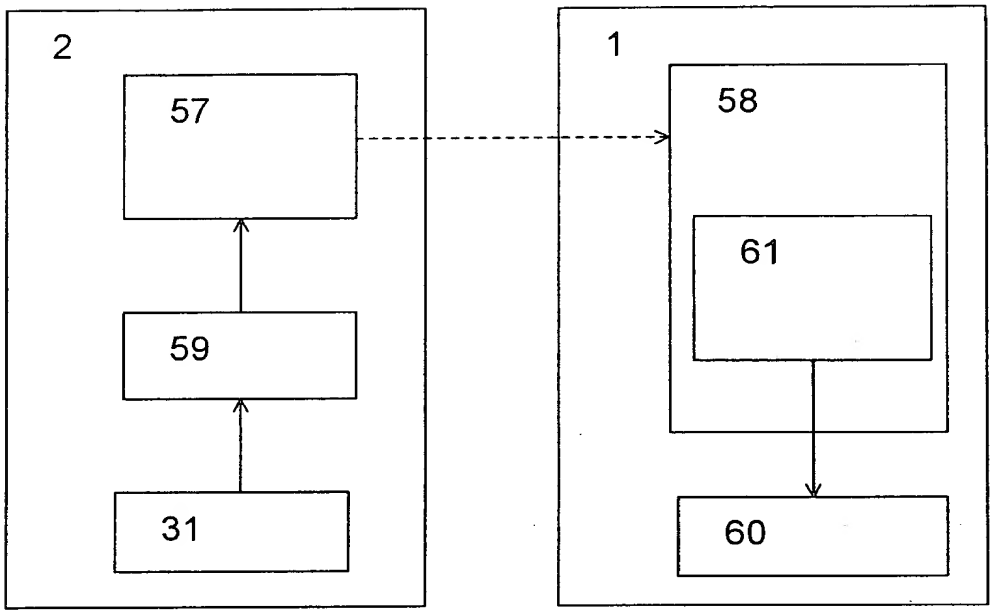
ФИГ. 2


2
30
32
37
38
31
41
34
36
35
33
39
40

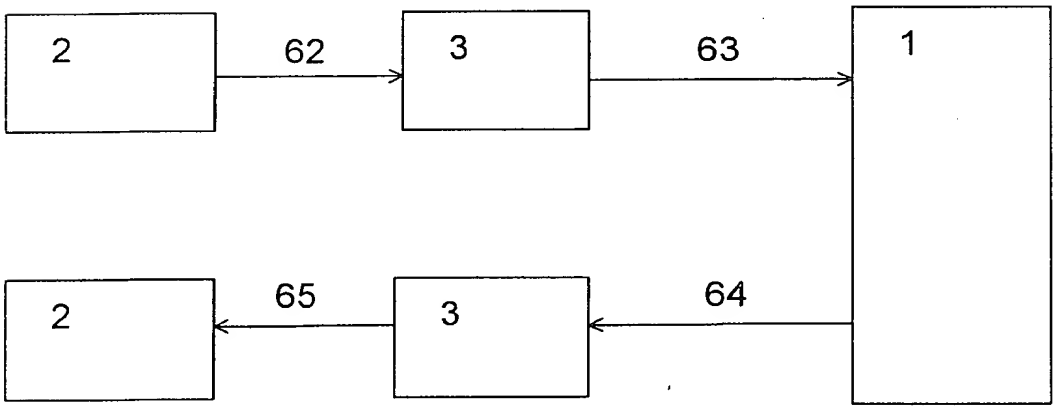
ФИГ. 3


2
42
49
51
50
45
46
1
43
52
18
54
31
22
44
56
55
48
47
53

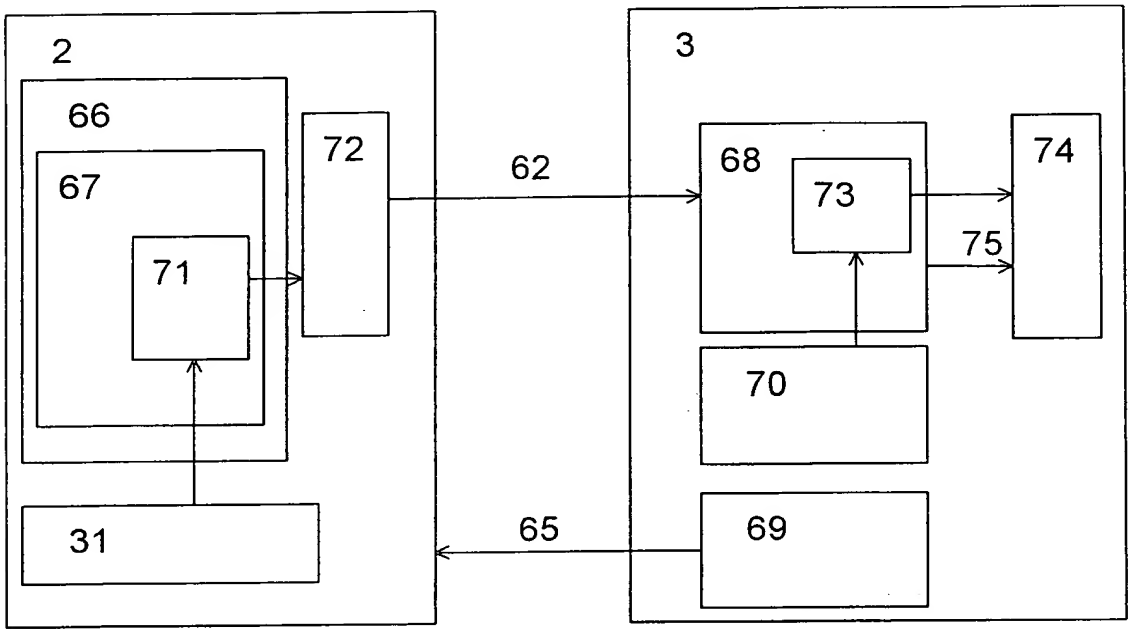
ФИГ. 4



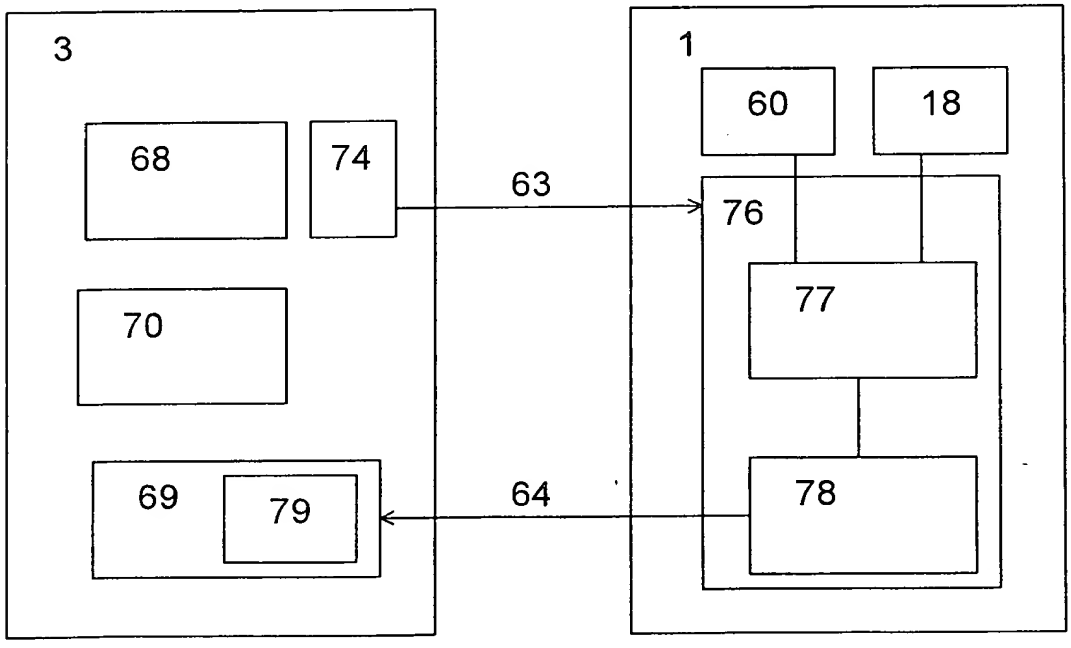
ФИГ. 5



ФИГ. 6


2
66
67
71
72
31
62
65
3
68
73
74
75
70
69

ФИГ. 7


3
68
74
70
69
79
63
64
1
60
18
76
77
78

ФИГ. 8

РЕФЕРАТ

к патенту № _____ по изобретению «Способ проведения платежей и устройство для его реализации (варианты)»

Изобретение относится к торговым системам, электронным системам массового обслуживания, платежным системам, коммуникационным системам, и может быть использовано для организации торговли ценными бумагами, для организации платежных систем и систем торговли на основе компьютерных сетей, для организации банков и банковских систем, магазинов, сервисных центров, лотерей и т.п.

Сущность изобретения состоит в новом способе проведения платежей, что позволяет, в отличие от известного уровня техники, при проведении платежей по открытым телекоммуникационным сетям обеспечить защиту денежных интересов каждого участника от злоупотреблений других участников, обеспечивает защиту приватности плательщиков и получателей, допускает платежи в диапазоне от микроплатежей до платежей бизнес-уровня, обеспечивает зависимость времени проведения платежа только от быстроты действия сетевых соединений, но не от суммы платежа, допускает возможность обслуживания оператором платежной системы клиентов, число которых растет пропорционально его ресурсам, допускает легкое встраивание в произвольную торговую систему, обеспечивает возможность каждого клиента как платить, так и принимать платежи, допускает возможность проведения платежей между клиентами различных банков.

Реализация способа проведения платежей осуществляется устройством.

8 с.п. ф-лы, 8 илл.